(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年8 月29 日 (29.08.2002)

PCT

(10) 国際公開番号
WO 02/067512 A1

(51) 国際特許分類[7]: H04L 12/56, 12/22

(21) 国際出願番号: PCT/JP02/01434

(22) 国際出願日: 2002 年2 月19 日 (19.02.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-041746 2001 年2 月19 日 (19.02.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒211-8588 神奈川県 川崎市中原区 上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 松平 直樹 (MATSUHIRA,Naoki) [JP/JP]; 〒211-8588 神奈川県 川崎市中原区 上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

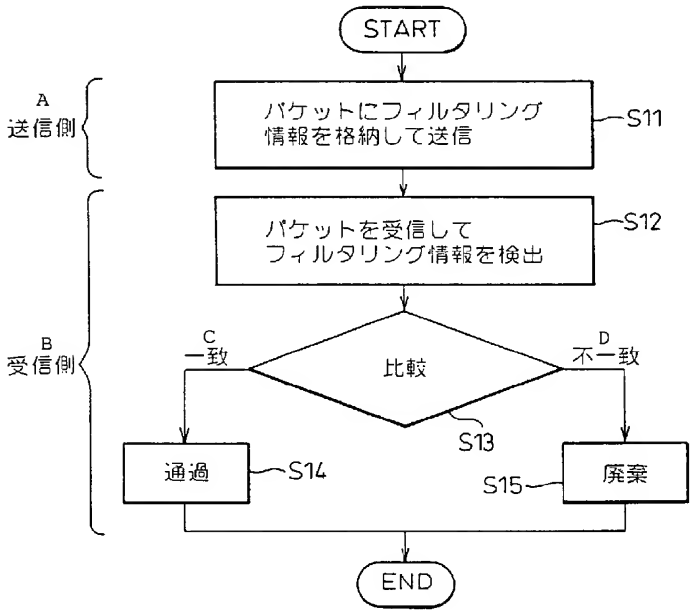
(74) 代理人: 石田 敬, 外(ISHIDA,Takashi et al.); 〒105-8423 東京都 港区虎ノ門三丁目５番１号 虎ノ門３７森ビル 青和特許法律事務所 Tokyo (JP).

(81) 指定国 (国内): JP, US.

[続葉有]

(54) Title: PACKET FILTERING METHOD AND PACKET COMMUNICATION SYSTEM FOR ENSURING COMMUNICATION SECURITY

(54) 発明の名称: 通信のセキュリティを確保するためのパケットフィルタリング方法およびパケット通信システム



A...TRANSMISSION SIDE
B...RECEIVING SIDE
S11...STORE FILTERING INFORMATION IN PACKET AND TRANSMIT IT
S!2...RECEIVE PACKET AND DETECT FILTERING INFORMATION
S13...COMPARE
C...AGREEMENT
D...DISAGREEMENT
S14...PASSAGE
S15...DISCARD

(57) Abstract: A packet filtering method adapted for simplifying filtering conditions and to the Ipsec. This method comprises (i) storing filtering information used for filtering, by the receiving sides, a packet to be transmitted to the receiving side and transmitting this information from the transmission side (S11), (ii) Receiving a packet from the transmissions side, extracting the filtering information stored in the packet (S12), and providing it for the filtering by the receiving side. This filtering information comprises simple filter keys (FK).

[続葉有]

WO 02/067512 A1

添付公開書類:
— 国際調査報告書

(57) 要約:

フィルタリングのためのフィルタ条件を簡素化すると共にＩＰｓｅｃにも対応可能なパケットフィルタリング方法を提供する。この方法においては、（ｉ）受信側に送信すべきパケットに、受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信し（Ｓ１１）、（ii）送信側からのパケットを受信し、該パケットに格納されたフィルタリング情報を検出して（Ｓ１２）、受信側でのフィルタリングに供する。このフィルタリング情報は単純なフィルタキー（ＦＫ）からなる。

明　細　書

通信のセキュリティを確保するためのパケットフィルタリング方法およびパケット通信システム

技術の分野

本発明は、インターネットにおいて通信のセキュリティを確保するための、パケットフィルタリング方法、そのための通信装置および認証装置、およびパケット通信システムに関する。

背景技術

フィルタリング技術は、企業等がインターネットに接続する場合に、該インターネットからの、または、インターネットへの不適切なアクセスを制限するための技術であり、通常、ファイアウォールやルータあるいはホスト等の通信装置にフィルタリング手段として実装される。このフィルタリング手段は、インターネットから上記企業等（またはこの逆）にアクセスする各パケットについて、予め定めた制限条件に合致するか否か判定を行い、合致したときは当該パケットを廃棄してしまう。

例えば、企業等内のイントラネットで使用されるプライベートアドレスは、企業内においてのみ自由に使えるアドレスであるから、このようなアドレスを含むパケットがインターネット上に転送されることは不適切であり、当該パケットを上記フィルタリング手段により廃棄する。あるいは、ある特定のアプリケーションについては予め特定のポート番号を指定しておいて、そのポート番号を含むパケットのみをフィルタリング手段でアクセスを許可する、ということが行われる。

図２０は本発明の対象となるネットワークを概略的に示す図である。

本図において、左側はＩＳＰ（Ｉｎｔｅｒｎｅｔ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ）により構築されるインターネットを表し、右側は企業のネットワーク例えばイントラネットを表す。そしてこれらの境界に配置されるのが通信装置であり、本発明は主としてこの通信装置を対象とする。

なお上記「通信装置」の語は、本発明において、前述したファイアウォールやルータあるいはホスト等を総称したものであり、この通信装置内でパケットフィルタリングが行われる。

図２１は従来の通信装置の一般的構成を表す図であり、

図２２は図２１の比較テーブル１２を詳細に示す図である。

図２１において、参照番号１０は上記の通信装置であり、具体的にはルータまたはホストである。

この通信装置１０内には、パケットフィルタリングを行うための比較手段１１が設けられる。この比較手段１１は比較テーブル１２を備え、この比較テーブル１２を参照しながら、入力（ＩＮ）されたパケットＰＫＴを通過させるか、または廃棄するか、を決定する。通過が許可されたパケットＰＫＴはＯＵＴより出力される。

上記の通過または廃棄のために参照される比較テーブル１２の詳細例を図２２に示す。

本図を参照すると、比較テーブル１２内には、フィルタ条件（＜１＞，＜２＞…＜ｋ＞）が予めリストとして格納されている。パケットＰＫＴが通信装置１０に入力されると、ＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）の場合、各パケット毎に、フィルタ条件である、「宛先ＩＰアドレス」、「発信ＩＰアドレス」、「宛先ポート番号」、「発信ポート番号」等がチェックされ、このフィルタ条

件に合致しないパケットＰＫＴは廃棄される。

上記比較テーブル１２の中で、「宛先ＩＰアドレスに対するマスク」とあるのは、例えば宛先ＩＰアドレス（ｍビット）のうち下位ｎ（ｍ＞ｎ）ビットはマスク（無視）することを意味する。このマスクにより、複数の通信相手を一つの集合体としてフィルタリングでき、効率がよい。同テーブル１２内の「発信ＩＰアドレスに対するマスク」も同様の目的で用いられる。

上記比較テーブル１２にて指定されるフィルタ条件の対象は、通常、各パケットのヘッダ内に記述される情報である。このヘッダについて以下に実際の例を示す。

図２３はＩＰｖ４ヘッダの実際の内容を示すフォーマット図、

図２４はＩＰｖ６ヘッダの実際の内容を示すフォーマット図、

図２５はＴＣＰヘッダの実際の内容を示すフォーマット図、

図２６はＵＤＰヘッダの実際の内容を示すフォーマット図である。

図２３のＩＰｖ４（ＩＰ　Ｖｅｒｓｉｏｎ　４）ヘッダを参照すると、上記「発信ＩＰアドレス」は“Ｓｏｕｒｃｅ　Ａｄｄｒｅｓｓ”によりチェックされ、上記「宛先ＩＰアドレス」は“Ｄｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓ”によりチェックされる。

図２４のＩＰｖ６（ＩＰ　Ｖｅｒｓｉｏｎ　６）ヘッダにおいても、上述の図２３の場合と同様である。

図２５のＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）ヘッダは、ＩＰよりも上位層で機能するが、前述と同様、上記「発信ポート番号」は“Ｓｏｕｒｃｅ　Ｐｏｒｔ”によりチェックされ、上記「宛先ポート番号」は“Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ”によりチェックされる。なおこのＤｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔは、特定のアプリケーションを指定するこ

とが多い。

図２６のＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）ヘッダにおいても、上述の図２５の場合と同様である。

上述した従来の比較手段１１（図２１）によると、次のような問題が生ずる。　第１には、今後益々通信相手の数が増大するのに伴って、上述したフィルタ条件の数も増大することである。すなわち、上記比較テーブル１２へのフィルタ条件のエントリ数が増大してしまい、ハードウエアの増大と共にフィルタリング時間も増大してしまう、という問題である。

第２は、今後その利用が拡大すると考えられるＩＰｓｅｃ（ＩＰＳｅｃｕｒｉｔｙ）プロトコルを導入した場合、上記の上位層のＴＣＰヘッダやＵＤＰヘッダが、そのＩＰｓｅｃにより暗号化されてしまい、図２５や図２６に示す“Ｓｏｕｒｃｅ　Ｐｏｒｔ”および“Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ”を用いたフィルタリングができなくなる、という問題である。

また付随的には、ＶｏＩＰ（Ｖｏｉｃｅ　ｏｖｅｒ　ＩＰ）等のように、ポート番号がネゴシエーションによりダイナミックに決定される、いわゆるピア・ツー・ピア型のアプリケーションでは、静的な設定でフィルタリングできず、その結果、セキュリティを確保するために、ＶｏＩＰのパケットを全てフィルタリングしなければならず、実質的にＶｏＩＰが使えない等の問題もある。

発明の開示

本発明は、上記問題点に鑑み、主として、フィルタ条件のエントリ数を大幅に削減すると共にＩＰｓｅｃにも対応可能な、パケットフィルタリング方法およびそのための通信装置を提供することを目的とするものである。

本発明は上記目的を達成するために、フィルタリングのためのフィルタ条件を簡素化すると共にＩＰｓｅｃにも対応可能なパケットフィルタリング方法を提供する。そしてこの方法は、

（ｉ）受信側に送信すべきパケットに、受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信するステップと、

（ii）送信側からのパケットを受信し、該パケットに格納されたフィルタリング情報を検出して、受信側でのフィルタリングに供するステップを含んでなる。そして、このフィルタリング情報は単純なフィルタキーからなる。

図面の簡単な説明

図１は、本発明に係るパケットフィルタリング方法を示すフローチャート、

図２は、ＴＣＰ／ＵＤＰヘッダを含む一般的なパケットを示す図、

図３は、ＩＰｓｅｃを採用した一般的なパケットを示す図、

図４は、従来のフィルタリングを採用した場合のパケットを示す図、

図５は、本発明に基づくフィルタキーを格納したパケットを示す図、

図６は、図５に示す本発明のパケットにＩＰｓｅｃを採用した場合のパケットを示す図、

図７は、ＩＰｖ６拡張ヘッダの実際の内容を示すフォーマット図、

図８は、本発明を適用したネットワークを図解的に表す図、

図９は、本発明に基づく、パケット受信側の通信装置の基本構成

を示す図、

図１０は、図９の通信装置の第１の具体例を示す図、

図１１は、図９の通信装置の第２の具体例を示す図、

図１２は、本発明の基づく、パケット送信側の通信装置の基本構成を示す図、

図１３は、図１２の通信装置の第１の具体例を示す図、

図１４は、図１２の通信装置の第２の具体例を示す図、

図１５は、本発明が適用されるパケット通信システムの概要を示す図、

図１６は、図１５に示す認証装置の基本構成を示す図、

図１７は、図１６に示す認証手段の具体的構成例を示す図、

図１８は、図１７のフィルタキー割当テーブル６７の一例を示す図、

図１９は、一連のフィルタキーの提供手続を表すシーケンス図、

図２０は、本発明の対象となるネットワークを概略的に示す図、

図２１は、従来の通信装置の一般的構成を表す図、

図２２は、図２１の比較テーブル１２を詳細に示す図、

図２３は、ＩＰｖ４ヘッダの実際の内容を示すフォーマット図、

図２４は、ＩＰｖ６ヘッダの実際の内容を示すフォーマット図、

図２５は、ＴＣＰヘッダの実際の内容を示すフォーマット図、

図２６は、ＵＤＰヘッダの実際の内容を示すフォーマット図、

図２７は、本発明を適用した具体的なネットワークを示す図である。

発明の実施の形態

図１は本発明に係るパケットフィルタリング方法を示すフローチャートである。

本図に示すステップＳ１１～Ｓ１５のうち、特に本発明を特徴づけるのはステップＳ１１およびＳ１２である。

ステップＳ１１：受信側に送信すべきパケットに、受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信する。

ステップＳ１２：送信側からのパケットを受信し、このパケットに格納された上記のフィルタリング情報を検出して、受信側でのフィルタリングに供する。

この受信側でのフィルタリングの動作（Ｓ１３～Ｓ１５）は従来と実質的に同じである

ステップＳ１３：受信側にて、予め定めた受信側のフィルタリング情報を保持し、パケットから検出された送信側のフィルタリング情報と受信側のフィルタリング情報とを比較する。

ステップＳ１４：上記の比較の結果、両者が一致したら当該パケットを通過させる。

ステップＳ１５：上記の比較の結果、両者が不一致のとき当該パケットを廃棄する。

上記のように本発明はフィルタ条件を、新たに定義したフィルタリング情報を用いて定めるようにした。このフィルタリング情報を構成するコードを本発明では、以下、フィルタキーと称する。

本発明は、図２２に示す従来の煩雑なフィルタ条件となるフィルタデータに代えて、あるいはその従来のフィルタデータと共に、単純なフィルタキーを用いる。そしてこのフィルタキーを上記の比較の対象とする。

従来との大きな相違は、フィルタ条件が従来、ユーザ一意（ｕｎｉｑｕｅ）に定められたのに対し、本発明では、ユーザを特定することなくパケット自体にフィルタ条件（フィルタキー）を埋め込ん

だことにある。

したがって、例えば、あるメーカの資材購買部門と、該部門に連携して独占的に資材を納入しているある下請メーカとの間では、単一の共通フィルタキーを割り当て、両者間の通信パケットに該共通フィルタキーを埋め込んでフィルタリングすることによりセキュリティを確保する、といったようなことが可能となる。これはフィルタ条件の数の大幅な削減をもたらす。

このように本発明は、通信同士間で予め定めた特定のフィルタキーを、当該通信に供する各パケットに埋め込んで、所期のフィルタリングを実現するが、この場合、そのフィルタキーを各パケットのどこに格納すべきか、という問題がある。

この問題の解決のために、本発明は、既述の第２の問題、すなわちＴＣＰヘッダあるいはＵＤＰヘッダが、ＩＰｓｅｃにより暗号化されて、フィルタリングができなくなるという問題も同時に解決することを企図して、次のような、フィルタキーの格納手法をとる。この格納手法に至る経緯を、以下の各図に沿って順次説明する。

図２はＴＣＰ／ＵＤＰヘッダを含む一般的なパケットを示す図である。

本図において、パケットＰＫＴの先頭にはＩＰヘッダが置かれ、続いて、ＴＣＰヘッダ（またはＵＤＰヘッダ）が置かれ、その後に本来のデータが続く。

図３はＩＰｓｅｃを採用した一般的なパケットを示す図である。

図２のパケットＰＫＴに対してＩＰｓｅｃを採用すると、ＩＰヘッダの直後にＩＰｓｅｃ暗号化ヘッダが置かれ、続くＴＣＰヘッダ（またはＵＤＰヘッダ）とデータとが暗号化（ハッチングで表す）されてしまい、既述の第２の問題を生じさせる。

図４は従来のフィルタリングを採用した場合のパケットを示す図

である。

図２２において説明したフィルタ条件は、パケットＰＫＴ内のＦ（ＩＰヘッダに対し）やＦ’（ＴＣＰまたはＵＤＰヘッダに対し）に設定される。

図５は本発明に基づくフィルタキーを格納したパケットを示す図である。

このパケットはＩＰｖ６に準拠したパケットであり、ＩＰｖ６拡張ヘッダ（ＥＸＴ）にフィルタキーＦＫとして格納される。あるいはそのＥＸＴにフィルタキーヘッダとして形成される。

またはＩＰｖ６ヘッダ内のフローラベル領域に、そのフィルタキーＦＫ’（点線で示す）が格納される。このフローラベル領域は、前述した図２４（ＩＰｖ６ヘッダ）の右上に、“Ｆｌｏｗ　Ｌａｂｅｌ”として既に示されている。この領域の利用態様についてはまだ定められていない。

図６は図５に示す本発明のパケットにＩＰｓｅｃを採用した場合のパケットを示す図である。

本図より明らかなように、ＩＰｓｅｃによりＴＣＰヘッダ（またはＵＤＰヘッダ）が暗号化されても、フィルタキーＦＫの方は全く影響を受けない。このフィルタキーＦＫが格納され、または、フィルタキーヘッダとして形成される前記ＩＰｖ６拡張ヘッダについて図示しておく。

図７はＩＰｖ６拡張ヘッダの実際の内容を示すフォーマット図である。

このＩＰｖ６拡張ヘッダは、ＩＰｖ６のオプション形式に準拠している。

本図に示すとおり、ＩＰｖ６拡張ヘッダＥＸＴは、フォーマット上、図２４に示すＩＰｖ６ヘッダに続けて配置されるもので、さら

に複数のＥＸＴをシリーズにつなげることができる。したがって図６に示すＩＰｓｅｃ暗号化ヘッダは、その複数のＥＸＴの１つとして配置することもできる。次のＥＸＴとの境界は、図７の“Ｈｄｒ　Ｅｘｔ　Ｌｅｎ”（ＥＸＴ長）により分かる。

フィルタキーＦＫは、そのＥＸＴの１つの中に格納することもできるし、あるいは、このＥＸＴそのものをフィルタキーヘッダとしてもよい。

図２４に示す“Ｎｅｘｔ　Ｈｅａｄｅｒ”をまず検出すると、ここにはそのフィルタキーが格納されている拡張領域のアドレスが書かれている。このアドレスのところをアクセスすれば、図７に表すように目的とするフィルタキー（ＦＫ）が示されている。なおこの拡張領域をどのように利用するかはユーザに任されている。

以上、図２以降の図面を参照して説明した事項を要約すると、次のとおりである。

（ｉ）パケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ部分においてフィルタリング情報（フィルタキーＦＫ，ＦＫ’）を格納するようにする。

（ii）パケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダＥＸＴに、フィルタリング情報（フィルタキーＦＫ）を格納するようにする。

（iii）パケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ内のフローラベル（Ｆｌｏｗ　Ｌａｂｅｌ）領域に、フィルタリング情報（フィルタキーＦＫ’）を格納するようにする。

図８は本発明を適用したネットワークを図解的に表す図である。

すなわち図２０に示すネットワークに本発明を適用した様子を例示するが、このために通信装置１０ａ～１０ｄがさらに描かれてい

る。

本図では、フィルタキーＦＫとして、ＦＫ＝０ｘ８７２６０ｆａ８７９ｃｂ９０を用いる（ただしこれは全くの一例である）。すなわち、ネットワーク（インターネット）とネットワーク（イントラネット）の境界に配置される通信装置１０ｃは、上記のＦＫを予め保持する。

今仮に通信装置１０ａと１０ｂが、通信装置１０ｄに対し、所定のパケットを送信したものとする。

このとき、通信装置１０ｂからの一連のパケットには上記フィルタキーＦＫが格納されている。このため、通信装置１０ｃが保持するフィルタキーと一致し、当該パケットは該装置１０ｃを通過して通信装置１０ｄに到達することができる。

一方、通信装置１０ａからの一連のパケットに格納されるフィルタキーＦＫは、上記のＦＫとは異なる（本図中、！を付して示し、！＝ＮＯＴである）。このため、該装置１０ａからの一連のパケットは、通信装置１０ｃにおいて、フィルタキーの不一致と判定され、廃棄される。なお、この判定を行うための比較手段については後述の図９に示す。ここで、一旦図２７を参照する。

図２７は、本発明を適用した具体的なネットワークを示す図である。企業のネットワーク２００は、本発明の機能を有する通信装置（ホスト）２１０等の他に、インターネット１００のエッジルータ１１０にアクセスするためのアクセス回線に接続されるルータ２２０で構成される。一方、出張先３００では、インターネット１００に対してＬＡＮケーブル又は電話線で接続されたルータ３２０（無線ＬＡＮ基地局、Ｌ２スイッチ、ハブ、ＡＤＳＬモデム、メディアコンバータなどでもよい）を介して、本発明が適用される通信装置３１０が配置される。この通信装置３１０としてはノートＰＣであ

ってもよく、この場合は、ＰＨＳやＰＤＣあるいはＷ－ＣＤＭＡ等のデータ通信カードを使用することになる。

またさらに、一般家庭４００、ホテル客室５００、無線ＬＡＮによるホットスポット６００から、本発明が適用された通信装置により、インターネット１００をアクセスすることができる。なお、企業のネットワーク２００内のルータ２２０に本発明を適用することも可能であり、この場合は、ルータ２２０で企業内の複数の通信装置のフィルタキーを管理できるため、通信装置２１０等には本発明を適用しない、という運用も可能である。

図９は本発明に基づく、パケット受信側の通信装置の基本構成を示す図である。すなわち、本図の通信装置１０は、パケットフィルタリングを実施するための手段を含むパケット受信側の通信装置例えばルータまたはホストであって、任意に定めたフィルタリング情報を、フィルタキーＦＫとして、パケットのＰＫＴのヘッダ部分において格納して送信側より送信されたパケットを受信し、このヘッダ部分よりフィルタキーＦＫを検出するフィルタキー検出部２０を備える。

さらに、フィルタキー検出部２０により検出した送信側のフィルタキーと、予め保持している受信側のフィルタキーとを比較して、両者が不一致か否かを判定し、不一致のときに当該受信パケットを廃棄するよう指示する比較手段２１を備える。

この比較手段２１は、フィルタキーＦＫをリストとして収容するフィルタキーテーブル２２を有する。

図１０は図９の通信装置の第１の具体例を示す図である。

この第１の具体例の通信装置１０は、前述のフィルタキー検出部２０をなすフィルタキーヘッダ検出部２３を通過した受信パケットＰＫＴを一時的に格納するバッファ２７を備える。ここに、前述の

比較手段２１は、

予め定めた複数の異なるフィルタキーＦＫ（＜１＞，＜２＞…＜ｋ＞）を保持するフィルタキーテーブル２２と、

フィルタキーヘッダ検出部２３により検出されたフィルタキーＦＫと一致するフィルタキーが、該フィルタキーテーブル２２内に有るか無いかを検索し、無しのときに廃棄指示を出力する検索部２５と、

上記の廃棄指示を受けて、バッファ２７内に格納されていたパケットを廃棄するように制御するバッファ制御部２６と、から構成される。

なおこの第１の具体例は、パケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダに、フィルタキーヘッダを形成する場合（図７）の構成を表している。

一方、パケットがＰＫＴがＩＰｖ６に準拠したパケットであって、そのＩＰｖ６ヘッダ内のフローラベル領域に、フィルタキーＦＫ’を格納する場合（図２４）の構成を図１１に示す。

図１１は図９の通信装置の第２の具体例を示す図である。

本図の構成は基本的に図１０の構成と同じである。相違する点は、フィルタキー検出部２０がフローラベル領域検出部２４となったこと、検出されたフィルタキーはＦＫ’（コードはＦＫと同じであるが、パケット内の格納場所が異なる）であること、の２点である。動作は図１０の場合と同じである。

図１２は本発明に基づく、パケット送信側の通信装置の基本構成を示す図である。すなわち、本図の通信装置１０は、パケットフィルタリングを実施するための手段を含むパケット送信側の通信装置例えばホストであって、任意に定めたフィルタリング情報を設定す

る設定部３１と、設定部３１より入力されたフィルタリング情報をフィルタキーＦＫとして保持するフィルタキー保持部３２と、保持されたフィルタキーＦＫを入力として、パケットＰＫＴのヘッダ部分においてフィルタキーを格納するフィルタキー格納手段３３と、を少なくとも有して構成される。フィルタキーとして、例えば、ＴＣＰやＵＤＰのポート番号をそのまま用いても良い。このような運用を行えば、ＩＰパケットがＩＰ　ＳＥＣ　ＥＳＰを用いて、暗号化された場合でも、アプリケーションのフィルタリングが可能になる。あるいは、ＶｏＩＰなどポート番号が固定されないアプリケーションの場合、ＶｏＩＰのデータであることを示す値を決定し、その値をフィルタキーとして用いても良い。このような運用を行えば、ＶｏＩＰのみを通過させるようなサービスが可能になる。なお設定部３１は例えばキーボードであり、ここからフィルタリング情報となるフィルタキーのコードが入力される。このフィルタキーは、ダイナミックなネゴシエーションで相手方から通知されてもよいし、また、システム管理者から入手してもよい。この場合、フィルタキーは、時間単位、日単位あるいは週単位で更新してもよい。

上記格納手段３３の具体例とその周辺部分について、以下に説明する。

図１３は図１２の通信装置の第１の具体例を示す図である。

この第１の具体例においては、パケットＰＫＴがＩＰｖ６に準拠したパケットであって、前述のフィルタキー格納手段３３は、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダに、フィルタキーヘッダを形成するフィルタキーヘッダ生成部４１である。このフィルタキーヘッダは図７に示すとおりである。

本図の通信装置１０（例えばホスト）は、実際にはその他の周辺部分を備えている。

まず、ＩＰｓｅｃ暗号化ヘッダ（図６参照）を生成する暗号化ヘッダ生成部４３であり、ＴＣＰヘッダまたはＵＤＰヘッダを生成する上位層ヘッダ生成部４４である。また、図１２に示す、受信側へ転送すべき「データ」を生成するためのデータ生成部４５がある。

さらに、上記のフィルタキーヘッダ生成部４１、暗号化ヘッダ生成部４３、上位層ヘッダ生成部４４およびデータ生成部４５からの各出力を入力として、受信側へのパケットＰＫＴを生成するパケット組立／暗号化部４６を有する。このパケット組立／暗号化部４６からのパケットの出力フォーマットは、図６に示すとおりである。

図１４は図１２の通信装置の第２の具体例を示す図である。

この第２の具体例においては、パケットＰＫＴがＩＰｖ６に準拠したパケットであって、前述のフィルタキー格納部３３は、そのＩＰｖ６ヘッダ内のフローラベル領域に、フィルタキーＦＫ’を格納するＩＰｖ６ヘッダ生成部４２である。このフィルタキーＦＫ’を収容する該フローラベル領域は図２４において“Ｆｌｏｗ　Ｌａｂｅｌ”として示したとおりである。

本図の通信装置１０もまた、図１３に示したのと同様、ＩＰｓｅｃ暗号化ヘッダを生成する暗号化ヘッダ生成部４３と、ＴＣＰヘッダまたはＵＤＰヘッダを生成する上位層ヘッダ生成部４４と、受信側へ転送すべきデータを生成するデータ生成部４５と、を有し、また、これらからの各出力を入力とするパケット組立／暗号化部４６を有する。

以上で本発明に係るフィルタリング方法および装置の詳細を明らかにしたので、次に、その本発明に係るフィルタリング方法および装置を実際に運用する際に必要とされるセキュリティの仕組みについて説明する。すなわち、ユーザ認証の手段である。

図１５は本発明が適用されるパケット通信システムの概要を示す

図である。

本図に示すシステム５０は、転送されるパケットに対してフィルタリングが行われるパケット通信システムであり、パケット送信装置５１と、パケット受信装置５２と、認証装置５３と、を備える。

ここに、パケット送信装置５１は、送信側より受信側に送信すべきパケットに、この受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信する。一方、パケット受信装置５２は、ネットワークを介してサーバおよびクライアント間で上記送信側からのパケットを受信し、その受信パケットに格納されたフィルタリング情報を検出して、上記受信側でのフィルタリングに供する。そしてこれら装置間を仲介する認証装置５３は、フィルタリングサービスを受けるユーザから入力されたユーザ認証情報を受信して、そのユーザの認証を行うと共に、その認証後に、そのユーザに対し、上記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布する。

このようなパケット通信システム５０は、次の（Ｉ）および（II）のように機能的に表すことができる。

（Ｉ）該システム５０は、ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムであって、ユーザ側の上記サーバまたはクライアントから上記ネットワークへのアクセスに際し使用される第１手段と第２手段とを備える。これらは、

（ｉ）ユーザ認証情報を受信して、ユーザの認証を行う第１手段と、

（ii）その認証後にこのユーザに対し上記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段である。

なお上記第１手段および第２手段は、例えば後述する図１６において、それぞれ、フィルタリング認証手段６１およびフィルタキー提供手段６２に相当するものである（後述する（II）のパケット通信システムについても同様）。

上述した、フィルタリング機能を有するパケット通信システム５０によれば、ネットワークへのアクセスに対してユーザ認証が可能となり、例えば、出張先からインターネットを介してその出張者が属する組織のネットワークへのアクセスが可能になったり、あるいは、ある出張先のローカルなネットワークからインターネットへのアクセスが可能になる。

（II）上記システム５０は、ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムであって、上記ネットワーク側のユーザから上記サーバまたはクライアントへのアクセスに際し使用される第１手段と第２手段を備える。これらは、

（ｉ）ユーザ認証情報を受信して、ユーザの認証を行う第１手段と、

（ii）その認証後にこのユーザに対し上記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段である。

上述した、フィルタリング機能を有するパケット通信システム５０によれば、サーバの提供するサービスに対する認証は、時間単位、日単位、週単位等で最初に１回行っておけば、その後は認証なしでフィルタキーを用いたアクセス制限が可能になる。

次に上記の認証装置５３を一層詳しく説明する。

図１６は図１５に示す認証装置の基本構成を示す図である。

本図に示すように認証装置５３（図１５）は、フィルタリング認

証手段６１とフィルタキー提供手段６２とを備える。

フィルタリング認証手段６１は、フィルタリングサービスを受けるユーザから入力されたユーザ認証情報ＡＩを受信して、そのユーザの認証を行う。またフィルタキー提供手段６２は、フィルタリング認証手段６１での認証後に、そのユーザに対し、ユーザ認証情報ＡＩに対応するフィルタリング情報としてのフィルタキーＦＫを割り当てて配布する。

図１７は図１６に示す認証手段の具体的構成例を示す図である。

本図の構成の上段側は、図１６のフィルタリング認証手段６１に相当し、その下段側は、フィルタキー提供手段６２に相当する。

すなわち、フィルタリング認証手段６１は、ユーザ認証情報ＡＩを予め登録したユーザ認証データベース（ＤＢ）６５と、受信バッファ６３に入力されバッファされたユーザ認証情報ＡＩの真偽を、このユーザ認証データベース６５を参照して判定する判定部６４と、から構成される。

一方、フィルタキー提供手段６２は、ユーザ認証情報（ＡＩ）対応に予め割り当てたフィルタキー（ＦＫ）を保持するフィルタキー割当テーブル６７と、上述の真偽が真であるとき、そのフィルタキー割当テーブル６７より対応のフィルタキーＦＫを、一旦送信バッファ６８にバッファして当該ユーザに対して送出するフィルタキー送出部６６と、から構成される。なお上記テーブル６７の一例は次のとおりである。

図１８は図１７のフィルタキー割当テーブル６７の一例を示す図である。

ただし、上述のユーザ認証情報ＡＩは、一例としてユーザＩＤおよびパスワードであるものとする。ユーザが使い慣れたコードや数字を用いれば、ユーザにとって便利である。

本テーブル６７の左欄ＡＩには、予め定めた複数のユーザ毎に予め定められたユーザＩＤとパスワードが登録されている。一方、その右欄には、各ユーザＩＤおよびパスワードに対応して予め割り当てられたフィルタキーのナンバー等が登録されている。

本テーブル６７の左欄ＡＩと同等の内容を有する認証情報ＡＩが登録されているユーザ認証データベース６５を参照して、図１７の左上に示すように入力されたＡＩが、該データベース６５の中のＡＩと一致するものと、図１７の判定部１７が判定すると、その一致したＡＩ（例えば図１８のＡＩの欄の２段目のＡＩとする）は、フィルタキー送出部６６に入力される。該送出部６６はフィルタキー割当テーブル６７より、そのＡＩに対応する同２段目のフィルタキー（この例では No.２）を割り出して、ユーザ側に提供する。

上述した一連のフィルタキーの提供手続を図解して示すと次のとおりである。

図１９は一連のフィルタキーの提供手続を表すシーケンス図である。

本図に示すシーケンスは、既述の図８に示すネットワーク構成を想定すると理解し易い。ただし、図８には認証装置５３に関係するハードウェア／ソフトウェアは全く示されていないが、この認証装置５３は、図８の中のどこかに存在していればよい。つまりその認証装置５３の存在場所は図８の中のどこでもよい。

もし特定的に言うならば、認証装置５３は、認証用サーバ、ファイアウォール、ルータおよびホストのうちの少なくとも１つの中に構築することができる。図１９のシーケンスは、認証装置５３を独立の認証用サーバとした場合について示すものである。

図１９において、最初にクライアント（ユーザ）と認証用サーバ（５３）との間で、ユーザＩＤとパスワードに関する認証手続が順

次行われる。

図１７等に示すフィルタリング認証手段６１とフィルタキー提供手段６２とにより、認証が認証用サーバにおいてなされて対応のフィルタキーＦＫが該認証サーバよりクライアントに配布されると、クライアントはこのフィルタキーＦＫを埋め込んだ送信パケットを、アクセス対象サーバに向け送信する。この場合、そのフィルタキーＦＫは上記認証を経ているので有効なものであり、通信装置（例えば図８の１０ｃ）を通過し、目標のサーバ（右端）にその送信パケットは到達できる。

なお上記の手続は、ＷＷＷで行ってもよい。

本発明に係るフィルタリング方法および装置を実際に運用するに当っては、さらに、上述したフィルタキーを具体的にどのように設定するか、ということも検討しておかなければならない。以下、これについていくつかの好適例を挙げる。

ａ）フィルタキーＦＫとして、ＴＣＰまたはＵＤＰのポート番号を用いる。

なお、ＴＣＰやＵＤＰについては、図２～図６や図２５および図２６において説明したとおりである。特に、上述のＴＣＰやＵＤＰのポート番号については、図２５および図２６において、発信ポート番号（Ｓｏｕｒｃｅ　Ｐｏｒｔ）および宛先ポート番号（Ｄｅｓｔｉｎａｔｉｏｎ　Ｐｏｒｔ）として示されている。

ポート番号は一般にファイル転送やＷｅｂ等のサービスの単位を表すものとして用いるが、本発明ではこのポート番号のコピーをフィルタキーとし用いる。このため例えば図７のごとく該フィルタキーを拡張領域内にＦＫとして埋め込む。

このようにポート番号をそのままフィルタキーとして用いれば、既述したＩＰｓｅｃによる暗号化が行われた場合でも、アプリケー

ション毎のフィルタリングが支障なく行える。

ｂ）既述したＶｏＩＰを用いてユーザ間で通信を行うとき、これらユーザ間で取り決めたＶｏＩＰを示す値を、フィルタキーＦＫとする。

上述したファイル転送やＷｅｂ等はポート番号で一意に特定されるが、ＶｏＩＰについてはこのようにポート番号でそのアプリケーションを特定できない。

したがって、ユーザ間でＶｏＩＰ通信を開始する前に動的にこの通信がＶｏＩＰであることを特定する必要がある。そこでユーザ間で取り決めた、ＶｏＩＰを示す値を、例えば図７のフィルタキーＦＫのように埋め込めば、ＶｏＩＰについてもフィルタリングが可能となる。

この場合、上記のＶｏＩＰを示す値は、通信相手方でＶｏＩＰであると認識させる作用と、本発明に係るフィルタリングのための作用の双方の作用を同時に果すことになる。

ｃ）ある特定の条件のもとでユーザに個別に個人ＩＤが割り当てられているとき、その個人ＩＤをフィルタキーＦＫとする。

このような個人ＩＤの具体例としては、ソフトウェアの使用許可を示す登録番号（シリアルナンバー）や、あるいは各会社毎の従業員番号等がある。

一般に上記ソフトウェアの登録番号は、新バージョンとなったソフトウェアをソフトウェアメーカがサーバからユーザに提供する場合、悪意のユーザからそのサーバへの不正なアクセスを防ぐ上で有効であり、日常的によく使われる認証情報（ＡＩ）である。これをフィルタキーとして利用するのも便利である。

また一般に従業員番号は各企業において必ず各従業員に割り当てられるものでるから、これをフィルタキーとして利用するのも便利

である。

以上述べたフィルタキーの設定（ａ），ｂ）およびｃ））は、既存のコードや番号等をそのまま利用してフィルタキーとするものである。しかし、そのフィルタキーを新たに定義して応用することによって、従来にないパケット通信サービスを実現することができる。以下の１）および２）にその例を挙げる。

１）ユーザがあるグループに属するユーザであるとき、そのグループを特定する共有ＩＤを予め定めて、その共有ＩＤをフィルタキーＦＫとする。

ここに言うあるグループとは、一例として、多数のユーザが集合する学会あるいは企業の会議を構成するグループである。

例えば上記の会議に参加する各ユーザにのみ、当該ネットワークをアクセスネットワークとして、インターネット等の外部ネットワークにアクセスを許可できるようなサービスが提供できれば、その会議の価値は一層高まる。

このような場合、上記の会議に参加する各ユーザに個別に別々のフィルタ条件（図２２参照）を設定する、というのが従来のフィルタリング手法である。しかしこれでは煩雑でかつ面倒である。

そこで本発明を用いることにより、上記の会議を特定する、参加ユーザ全員に共通の共有ＩＤを、１つ設定して、その共有ＩＤをこれら全員に予め配布するようにする。そうすれば、きわめて簡単にグループ単位（会議毎）でのフィルタリングを行うことができる。

２）複数のユーザに同時にマルチキャストパケットが配信されるとき、そのマルチキャストパケットにより提供されるコンテンツを利用することが許可されたユーザのみに予め告知された利用者ＩＤを、フィルタキーＦＫとする。

例えば映画配信業者が多数のユーザに映画を同時に配信するよう

な場合、マルチキャストパケットが用いられる。しかしそのマルチキャストパケットは、他に何らかのゲート手段がない限り、全てのユーザに到達し、無料でそのコンテンツを提供してしまうことになる。

そこで本発明を用いることにより、きわめて簡単に、受信料を支払ったユーザに対してのみ選択的にそのコンテンツを提供することが可能となる。

すなわち、上記のフィルタキーＦＫとして、上記コンテンツ（映画等）を利用することが許可されたユーザすなわち受信料支払い済みのユーザのみに共通に告知された同一の利用者ＩＤを用いるようにする。そうすれば、この利用者ＩＤを知っているユーザのみがそのコンテンツを利用することができる。なお、その告知の手段は、Ｗｅｂでも電話でもＦＡＸでもよい。

上記の利用形態をさらに発展させると、上記の共通の利用者ＩＤを複数種用意して、上記映画配信業者が提供する複数種の映画番組に対してそれぞれの利用者ＩＤを個別に割り当てれば、個々の映画の番組毎に、受信料を支払ったユーザにのみ、所望の映画を配信することができる。

最後に、既述の図１５を再び参照して、本図においてＩＰｖ６のパケットを用いる場合の説明を付け加えると次のとおりである。ただし、既に図５および図７を用いて説明した内容と同じである。すなわち、パケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６拡張ヘッダに、フィルタリング情報を格納するようにする。

同様にパケットＰＫＴがＩＰｖ６に準拠したパケットであるとき、ＩＰｖ６拡張ヘッダに代えて、そのＩＰｖ６ヘッダ内のフローラベル領域に、フィルタリング情報を格納するようにする。

以上述べた本発明の実施の態様は、以下の付記のとおりである。

（付記１）受信側に送信すべきパケットに、受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信することを特徴とするパケットフィルタリング方法。

（付記２）送信側からのパケットを受信し、該パケットに格納されたフィルタリング情報を検出して、受信側でのフィルタリングに供することを特徴とするパケットフィルタリング方法。

（付記３）受信側にて、予め定めた受信側のフィルタリング情報を保持し、前記パケットから検出された送信側のフィルタリング情報と前記受信側のフィルタリング情報とを比較して両者が不一致のとき当該パケットを廃棄することを特徴とする付記２に記載のパケットフィルタリング方法。

（付記４）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ部分において前記フィルタリング情報を格納することを特徴とする付記１または２に記載のパケットフィルタリング方法。

（付記５）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダに、前記フィルタリング情報を格納することを特徴とする付記１または２に記載のパケットフィルタリング方法。

（付記６）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ内のフローラベル領域に、前記フィルタリング情報を格納することを特徴とする付記１または２に記載のパケットフィルタリング方法。

（付記７）パケットフィルタリングを実施するための手段を含むパケット送信側の通信装置であって、

任意の定めたフィルタリング情報を設定する設定部と、

前記設定部より入力された前記フィルタリング情報をフィルタキーとして保持するフィルタキー保持部と、

保持された前記フィルタキーを入力として、パケットのヘッダ部分においてフィルタキーを格納するフィルタキー格納手段と、を少なくとも有してなることを特徴とする通信装置。

（付記８）前記パケットがＩＰｖ６に準拠したパケットであるとき、前記フィルタキー格納手段は、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダに、フィルタキーヘッダを形成するフィルタキーヘッダ生成部であることを特徴とする付記７に記載の通信装置。

（付記９）ＩＰｓｅｃ暗号化ヘッダを生成する暗号化ヘッダ生成部と、

ＴＣＰヘッダまたはＵＤＰヘッダを生成する上位層ヘッダ生成部と、

受信側へ転送すべきデータを生成するデータ生成部と、をさらに有することを特徴とする付記８に記載の通信装置。

（付記１０）前記フィルタキーヘッダ生成部、前記暗号化ヘッダ生成部、前記上位層ヘッダ生成部および前記データ生成部からの各出力を入力として、受信側へのパケットを生成するパケット組立／暗号化部をさらに有することを特徴とする付記９に記載の通信装置。

（付記１１）前記パケットがＩＰｖ６に準拠したパケットであるとき、前記フィルタキー格納部は、そのＩＰｖ６ヘッダ内のフローラベル領域に、前記フィルタキーを格納するＩＰｖ６ヘッダ生成部であることを特徴とする付記７に記載の通信装置。

（付記１２）ＩＰｓｅｃ暗号化ヘッダを生成する暗号化ヘッダ生成部と、

ＴＣＰヘッダまたはＵＤＰヘッダを生成する上位層ヘッダ生成部と、

受信側へ転送すべきデータを生成するデータ生成部と、をさらに有することを特徴とする付記１１に記載の通信装置。

（付記１３）前記フィルタキーヘッダ生成部、前記暗号化ヘッダ生成部、前記上位層ヘッダ生成部および前記データ生成部からの各出力を入力として、受信側へのパケットを生成するパケット組立／暗号化部をさらに有することを特徴とする付記１２に記載の通信装置。

（付記１４）パケットフィルタリングを実施するための手段を含むパケット受信側の通信装置であって、

任意に定めたフィルタリング情報を、フィルタキーとして、パケットのヘッダ部分において格納して送信側より送信されたパケットを受信し、該ヘッダ部分より該フィルタキーを検出するフィルタキー検出部と、

前記フィルタキー検出部により検出した送信側のフィルタキーと予め保持している受信側のフィルタキーとを比較して、両者が不一致か否かを判定し、不一致のときに当該受信パケットを廃棄するよう指示する比較手段と、を備えることを特徴とする通信装置。

（付記１５）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダに付加されるＩＰｖ６拡張ヘッダに、前記フィルタキーヘッダを形成することを特徴とする付記１４に記載の通信装置。

（付記１６）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ内のフローラベル領域に、前記フィルタキーヘッダを格納することを特徴とする付記１４に記載の通信装置。

（付記１７）前記フィルタキー検出部を通過した受信パケットを一時的に格納するバッファを備えると共に、前記比較手段は、

予め定めた複数の異なるフィルタキーを保持するフィルタキーテーブルと、

前記フィルタキー検出部により検出されたフィルタキーと一致するフィルタキーが該フィルタキーテーブル内に有るか無いかを検索し、無しのときに廃棄指示を出力する検索部と、

前記廃棄指示を受けて、前記バッファ内に格納されていたパケットを廃棄するように制御するバッファ制御部と、からなることを特徴とする付記１４に記載の通信装置。

（付記１８）フィルタリングサービスを受けるユーザから入力されたユーザ認証情報を受信して、該ユーザの認証を行うフィルタリング認証手段と、

前記フィルタリング認証手段での認証後に、該ユーザに対し、前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布するフィルタキー提供手段と、

を有することを特徴とする認証装置。

（付記１９）前記フィルタリング認証手段は、

前記ユーザ認証情報を予め登録したユーザ認証データベースと、

前記の入力されたユーザ認証情報の真偽を、該ユーザ認証データベースを参照して判定する判定部と、を有してなり、

前記フィルタキー提供手段は、

前記ユーザ認証情報対応に予め割り当てた前記フィルタキーを保持するフィルタキー割当テーブルと、

前記の真偽が真であるとき、前記フィルタキー割当テーブルより対応の前記フィルタキーを、前記ユーザに対して送出するフィルタキー送出部と、を有してなることを特徴とする付記１８に記載の認

証装置。

（付記２０）前記認証装置は、

認証用サーバ、ファイアウォール、ルータおよびホストのうちの少なくとも１つの中に構築されることを特徴とする付記１８に記載の認証装置。

（付記２１）前記ユーザ認証情報は、ユーザＩＤおよびパスワードであることを特徴とする付記１８に記載の認証装置。

（付記２２）前記フィルタキーとして、ＴＣＰまたはＵＤＰのポート番号を用いることを特徴とする付記１８に記載の認証装置。

（付記２３）ＶｏＩＰを用いてユーザ間で通信を行うとき、該ユーザ間で取り決めたＶｏＩＰを示す値を、前記フィルタキーとすることを特徴とする付記１８に記載の認証装置。

（付記２４）ある特定の条件のもとで前記ユーザに個別に個人ＩＤが割り当てられているとき、その個人ＩＤを前記フィルタキーとすることを特徴とする付記１８に記載の認証装置。

（付記２５）前記ユーザがあるグループに属するユーザであるとき、該グループを特定する共有ＩＤを予め定めて、その共有ＩＤを前記フィルタキーとすることを特徴とする付記１８に記載の認証装置。

（付記２６）複数のユーザに同時にマルチキャストパケットが配信されるとき、該マルチキャストパケットにより提供されるコンテンツを利用することが許可されたユーザにのみ予め告知された利用者ＩＤを、前記フィルタキーとすることを特徴とする付記１８に記載の認証装置。

（付記２７）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６拡張ヘッダに、前記フィルタリング情報を格納することを特徴とする付記１８に記載の認証装置。

（付記２８）前記パケットがＩＰｖ６に準拠したパケットであるとき、そのＩＰｖ６ヘッダ内のフローラベル領域に、前記フィルタリング情報を格納することを特徴とする付記１８に記載の認証装置。

（付記２９）転送されるパケットに対してフィルタリングが行われるパケット通信システムにおいて、

受信側に送信すべきパケットに、該受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信するパケット送信装置と、

ネットワークを介してサーバおよびクライアント間で前記送信側からのパケットを受信し、その受信パケットに格納された前記フィルタリング情報を検出して、前記受信側でのフィルタリングに供するパケット受信装置と、

前記フィルタリングサービスを受けるユーザから入力されたユーザ認証情報を受信して、該ユーザの認証を行うと共に、その認証後に、該ユーザに対し、前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布する認証装置と、

を備えることを特徴とするパケット通信システム。

（付記３０）ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムにおいて、

ユーザ側の前記サーバまたはクライアントから前記ネットワークへのアクセスに際し使用される手段であって、

ユーザ認証情報を受信して、該ユーザの認証を行う第１手段と、

その認証後に該ユーザに対し前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段と、

を備えることを特徴とするパケット通信システム。

（付記３１）ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムにおいて、

前記ネットワーク側のユーザから前記サーバまたはクライアントへのアクセスに際し使用される手段であって、

ユーザ認証情報を受信して、該ユーザの認証を行う第１手段と、

その認証後に該ユーザに対し前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段と、

を備えることを特徴とするパケット通信システム。

以上説明したように本発明によれば、次のような効果が得られる。

（１）フィルタ条件を示すテーブルには、フィルタキーのみを格納するだけでよく、しかも、そのフィルタキーは各ユーザ対応（つまり関係する全ての端末のＩＰアドレス対応）でなく特定のグループ対応で設定することができるので、上記のテーブルへのフィルタキーの設定、すなわちエントリは大幅に簡略化される。また、そのテーブルのメモリ容量は大幅に縮小できる。

従来は、図２２に示すフィルタ条件の説明から明白なように、多種のフィルタ条件データがあるため、比較の条件（ＡＮＤまたはＯＲ）が複雑になるが、本発明では上記のように、テーブルに格納されるのはフィルタキーのみであり、比較のための論理処理は飛躍的に簡素化され、このためフィルタリング処理は格段に高速化される。

（２）ＩＰｓｅｃプロトコルが導入されると、従来の、ＴＣＰヘッダまたはＵＤＰヘッダ内のフィルタ条件を用いたパケットフィル

タリングの実施はこれらヘッダの暗号化により不可能になるが、本発明によれば、これらＴＣＰヘッダまたはＵＤＰヘッダが暗号化されても、図６に示すとおり、フィルタキーはその暗号化の対象から外れるので、該パケットフィルタリングの実施に何の支障もない。

したがって、ポート番号の値が不定となるようなアプリケーションに対応する場合、あるいは、ポート番号の値が暗号化により不明となる場合に、全てのパケットの通過を禁止するのではなく、必要なパケット以外のパケットを廃棄するフィルタリングを実施するようにすることができる。

（３）従来苦手としてきた、ＶｏＩＰのようなアプリケーションに対しても、容易にパケットフィルタリングを適用可能となる。

（４）多数のユーザが参加する学会や会議等のグループ単位でのパケットフィルタリングが簡単に行える。

（５）映画の配信等のマルチキャストコンテンツに対し、受信料の支払いの有無に応じたユーザへの選択的な配信を簡単に行うことができる。

請　求　の　範　囲

１．受信側に送信すべきパケットに、受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信することを特徴とするパケットフィルタリング方法。

２．送信側からのパケットを受信し、該パケットに格納されたフィルタリング情報を検出して、受信側でのフィルタリングに供することを特徴とするパケットフィルタリング方法。

３．パケットフィルタリングを実施するための手段を含むパケット送信側の通信装置であって、

任意の定めたフィルタリング情報を設定する設定部と、

前記設定部より入力された前記フィルタリング情報をフィルタキーとして保持するフィルタキー保持部と、

保持された前記フィルタキーを入力として、パケットのヘッダ部分においてフィルタキーを格納するフィルタキー格納手段と、を少なくとも有してなることを特徴とする通信装置。

４．パケットフィルタリングを実施するための手段を含むパケット受信側の通信装置であって、

任意に定めたフィルタリング情報を、フィルタキーとして、パケットのヘッダ部分において格納して送信側より送信されたパケットを受信し、該ヘッダ部分より該フィルタキーを検出するフィルタキー検出部と、

前記フィルタキー検出部により検出した送信側のフィルタキーと予め保持している受信側のフィルタキーとを比較して、両者が不一致か否かを判定し、不一致のときに当該受信パケットを廃棄するよう指示する比較手段と、を備えることを特徴とする通信装置。

５．前記フィルタキー検出部を通過した受信パケットを一時的に

格納するバッファを備えると共に、前記比較手段は、

予め定めた複数の異なるフィルタキーを保持するフィルタキーテーブルと、

前記フィルタキー検出部により検出されたフィルタキーと一致するフィルタキーが該フィルタキーテーブル内に有るか無いかを検索し、無しのときに廃棄指示を出力する検索部と、

前記廃棄指示を受けて、前記バッファ内に格納されていたパケットを廃棄するように制御するバッファ制御部と、からなることを特徴とする請求項４に記載の通信装置。

６．フィルタリングサービスを受けるユーザから入力されたユーザ認証情報を受信して、該ユーザの認証を行うフィルタリング認証手段と、

前記フィルタリング認証手段での認証後に、該ユーザに対し、前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布するフィルタキー提供手段と、

を有することを特徴とする認証装置。

７．前記フィルタリング認証手段は、

前記ユーザ認証情報を予め登録したユーザ認証データベースと、

前記の入力されたユーザ認証情報の真偽を、該ユーザ認証データベースを参照して判定する判定部と、を有してなり、

前記フィルタキー提供手段は、

前記ユーザ認証情報対応に予め割り当てた前記フィルタキーを保持するフィルタキー割当テーブルと、

前記の真偽が真であるとき、前記フィルタキー割当テーブルより対応の前記フィルタキーを、前記ユーザに対して送出するフィルタキー送出部と、を有してなることを特徴とする請求項６に記載の認証装置。

８．転送されるパケットに対してフィルタリングが行われるパケット通信システムにおいて、

受信側に送信すべきパケットに、該受信側でのフィルタリングに供するためのフィルタリング情報を格納して送信側より送信するパケット送信装置と、

ネットワークを介してサーバおよびクライアント間で前記送信側からのパケットを受信し、その受信パケットに格納された前記フィルタリング情報を検出して、前記受信側でのフィルタリングに供するパケット受信装置と、

前記フィルタリングサービスを受けるユーザから入力されたユーザ認証情報を受信して、該ユーザの認証を行うと共に、その認証後に、該ユーザに対し、前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布する認証装置と、

を備えることを特徴とするパケット通信システム。

９．ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムにおいて、

ユーザ側の前記サーバまたはクライアントから前記ネットワークへのアクセスに際し使用される手段であって、

ユーザ認証情報を受信して、該ユーザの認証を行う第１手段と、

その認証後に該ユーザに対し前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段と、

を備えることを特徴とするパケット通信システム。

１０．ネットワークを介しサーバおよびクライアント間で転送されるパケットに対してフィルタリングサービスが行われるパケット通信システムにおいて、

前記ネットワーク側のユーザから前記サーバまたはクライアントへのアクセスに際し使用される手段であって、

ユーザ認証情報を受信して、該ユーザの認証を行う第１手段と、

その認証後に該ユーザに対し前記ユーザ認証情報に対応するフィルタリング情報としてのフィルタキーを割り当てて配布することによりアクセス制限を行う第２手段と、

を備えることを特徴とするパケット通信システム。

Fig.1

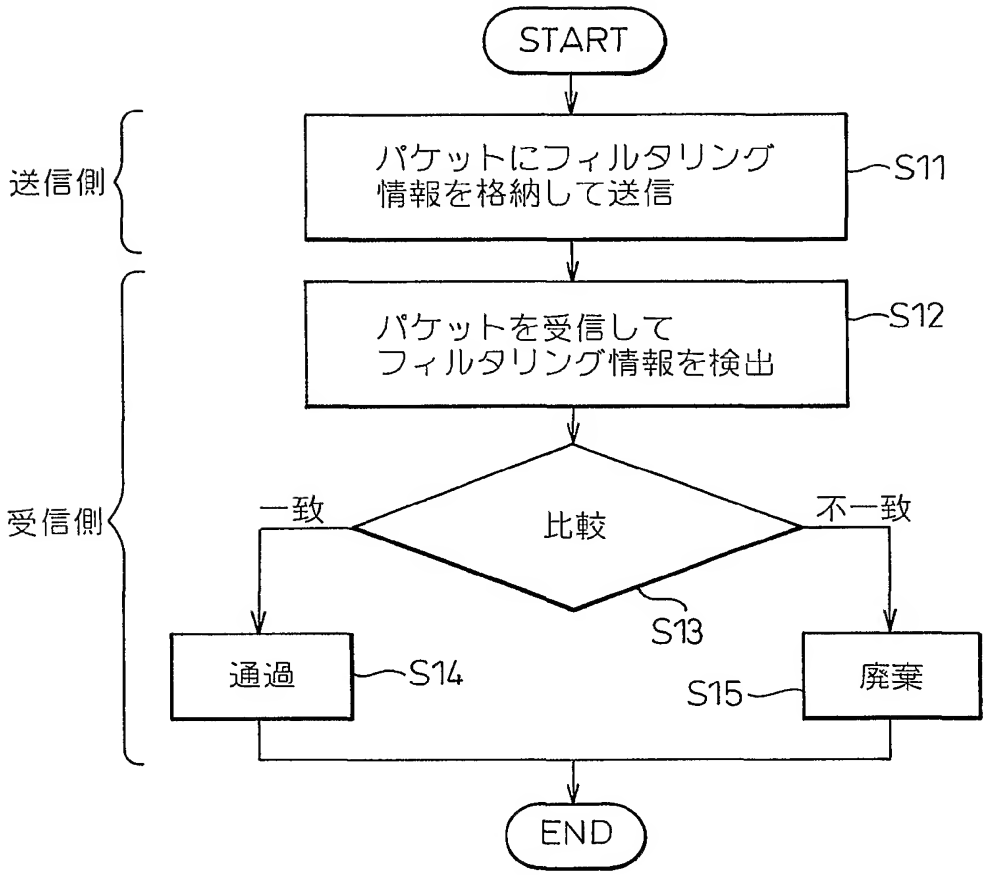

START
送信側
パケットにフィルタリング情報を格納して送信
S11
パケットを受信してフィルタリング情報を検出
S12
受信側
一致
比較
不一致
S13
通過
S14
S15
廃棄
END

Fig.2

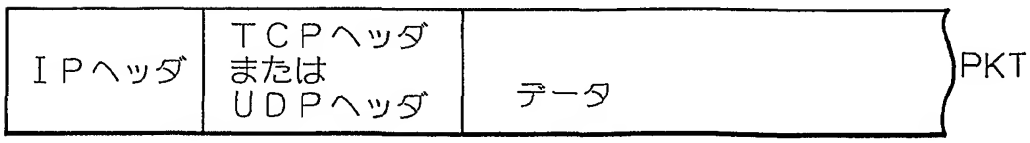

IPヘッダ
TCPヘッダまたはUDPヘッダ
データ
PKT

Fig.3

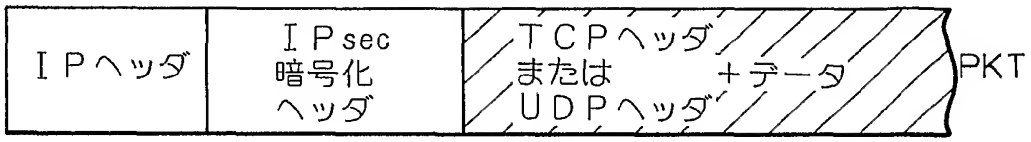


Fig.4

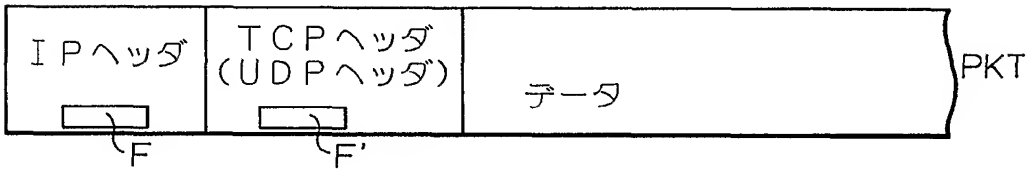


Fig.5

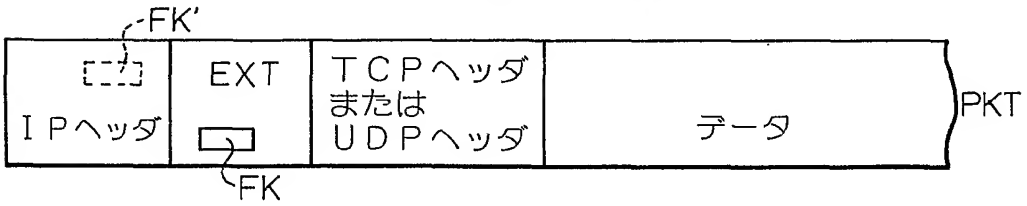


Fig.6

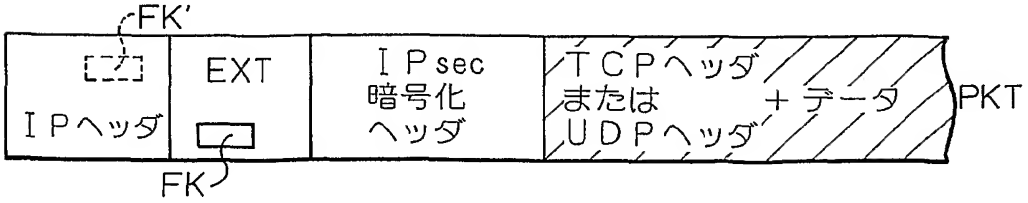


Fig.7

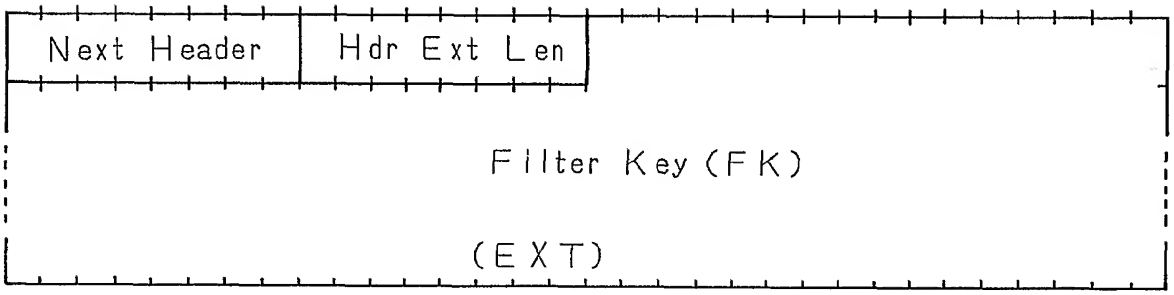


Fig.8

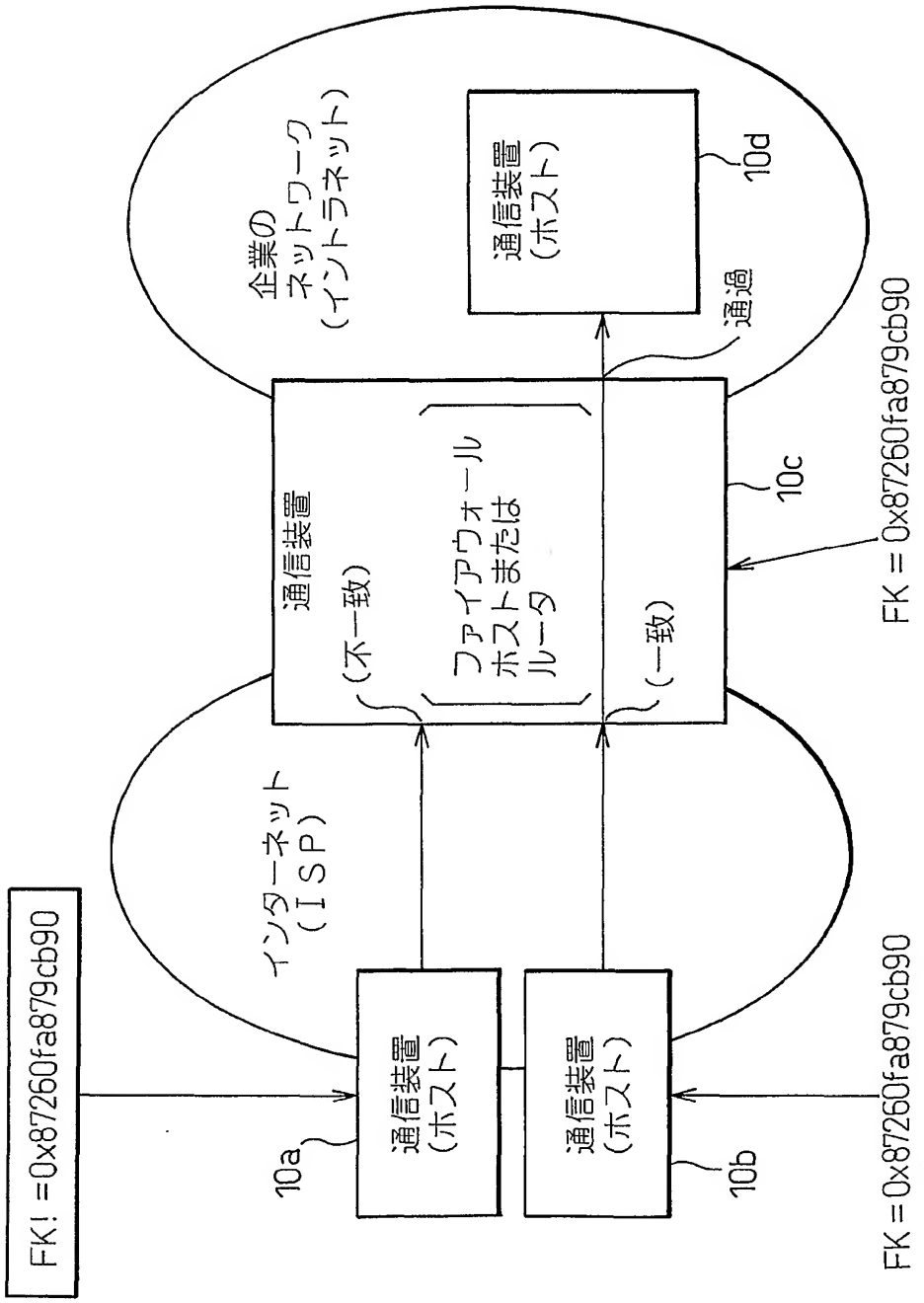

FK! =0x87260fa879cb90
インターネット
(ISP)
通信装置
(ホスト)
10a
通信装置
(ホスト)
10b
通信装置
(不一致)
ファイアウォール
ホストまたは
ルータ
(一致)
10c
企業の
ネットワーク
(イントラネット)
通信装置
(ホスト)
10d
通過
FK = 0x87260fa879cb90
FK = 0x87260fa879cb90

Fig.9

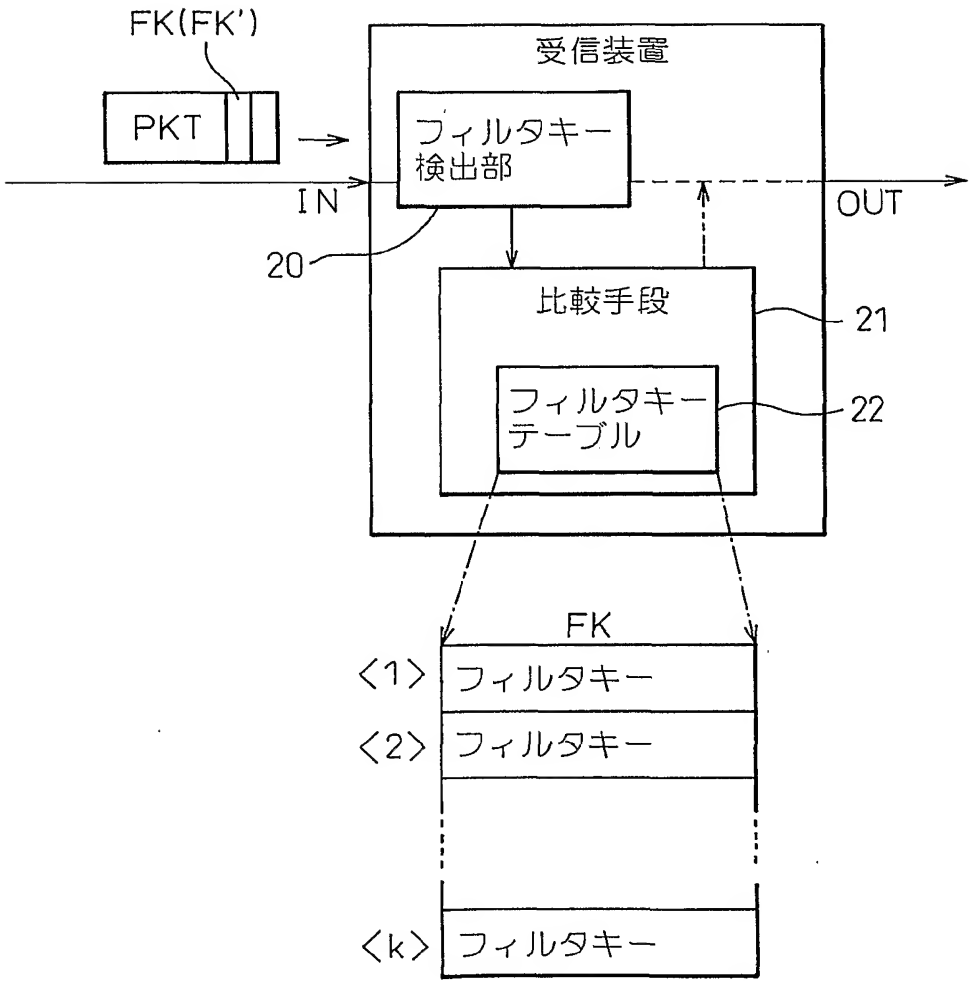

FK(FK')
PKT
受信装置
フィルタキー
検出部
IN
OUT
20
比較手段
21
フィルタキー
テーブル
22
FK
<1>
フィルタキー
<2>
フィルタキー
<k>
フィルタキー

Fig.10

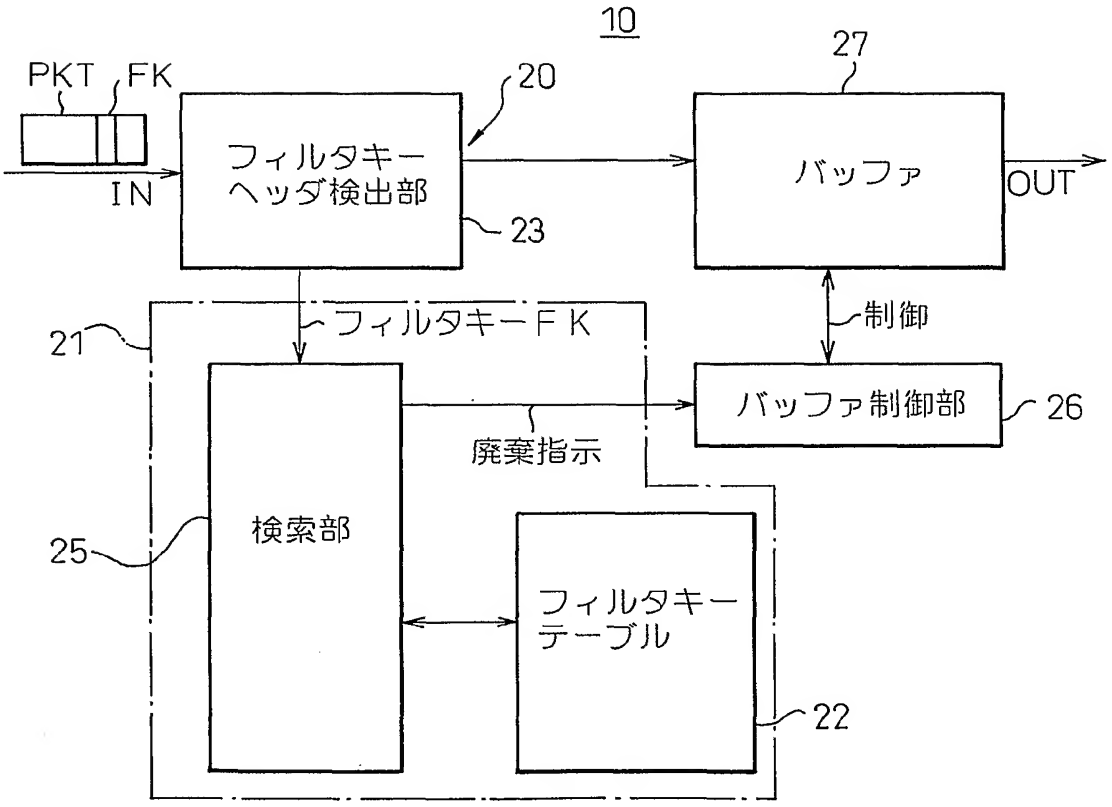

10
27
PKT
FK
20
フィルタキー
ヘッダ検出部
バッファ
OUT
IN
23
フィルタキーＦＫ
制御
21
バッファ制御部
26
廃棄指示
検索部
25
フィルタキー
テーブル
22

Fig.11

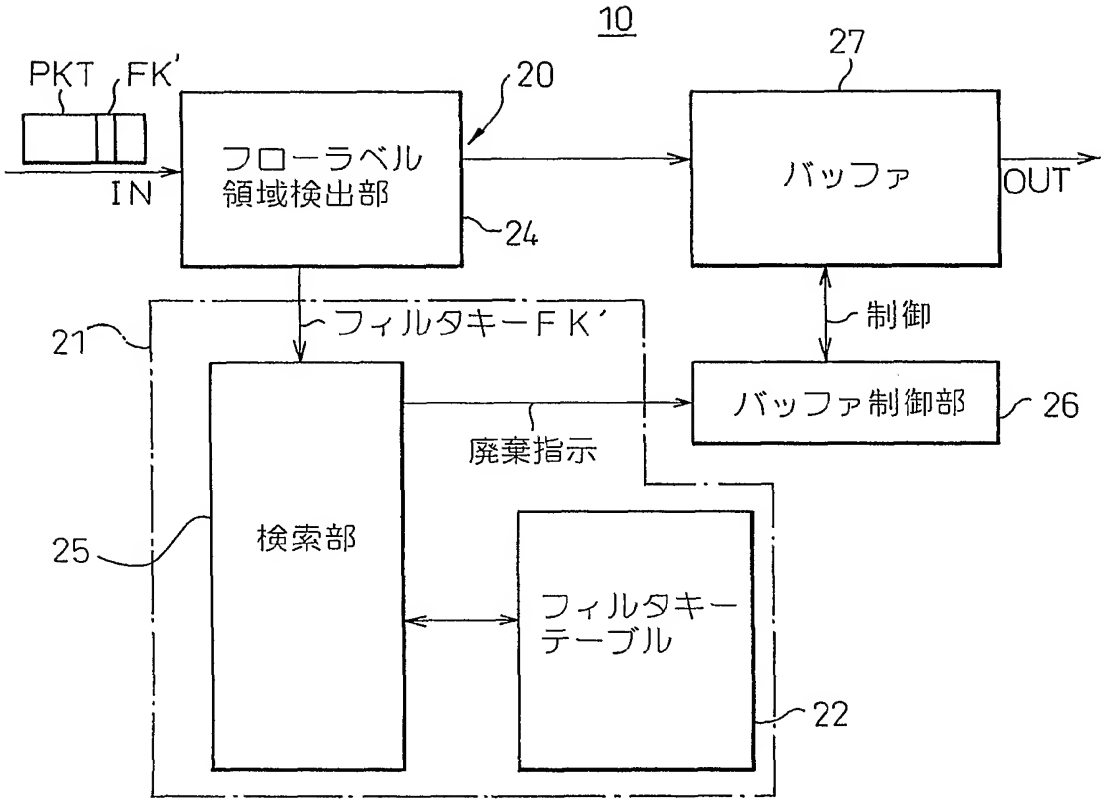

10
27
PKT
FK'
20
フローラベル
領域検出部
バッファ
OUT
IN
24
制御
フィルタキーFK'
21
バッファ制御部
26
廃棄指示
検索部
25
フィルタキー
テーブル
22

Fig.12

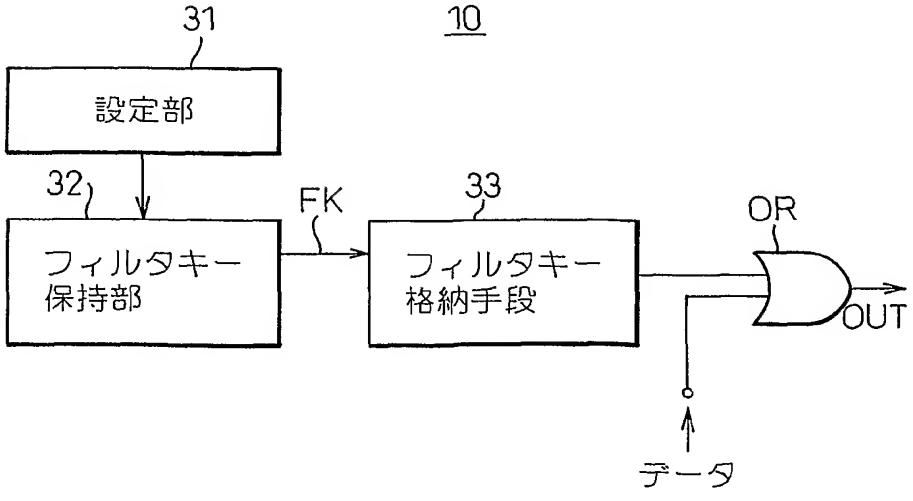

31
10
設定部
32
FK
33
OR
フィルタキー
保持部
フィルタキー
格納手段
OUT
データ

Fig.13

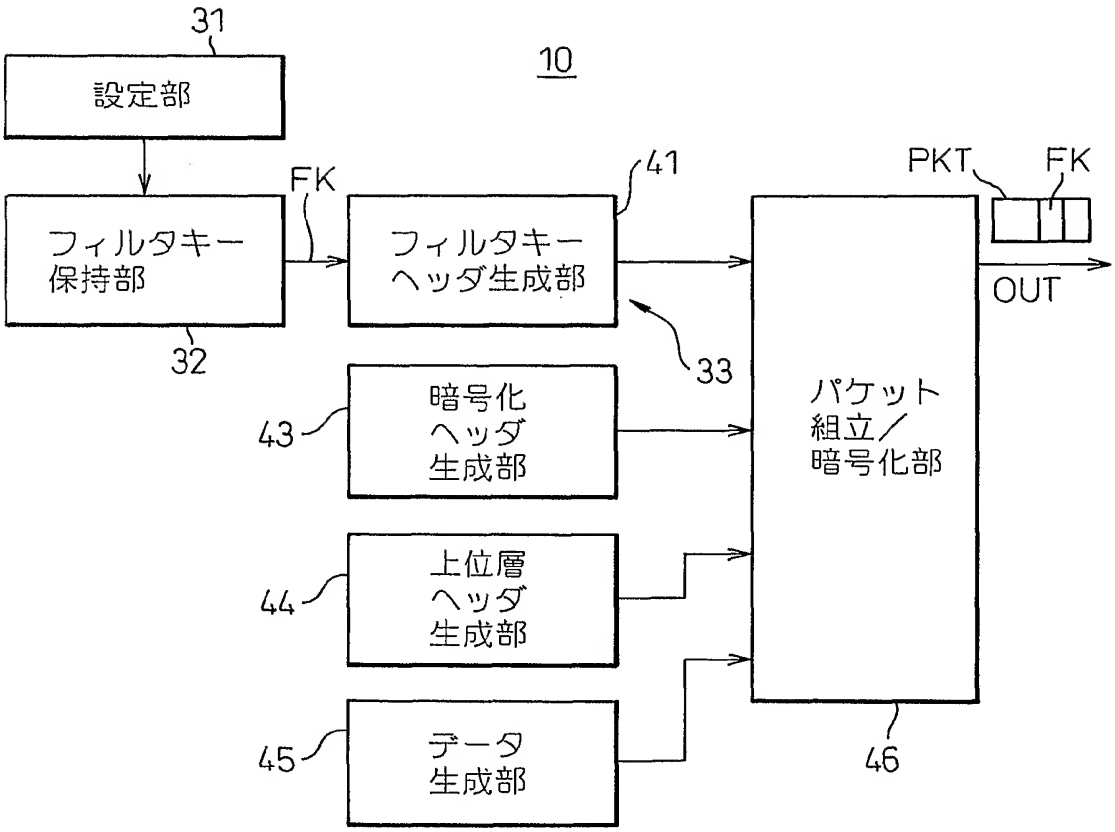

31
10
設定部
FK
41
PKT
FK
フィルタキー
保持部
フィルタキー
ヘッダ生成部
OUT
32
33
暗号化
ヘッダ
生成部
43
パケット
組立／
暗号化部
上位層
ヘッダ
生成部
44
データ
生成部
45
46

Fig.14

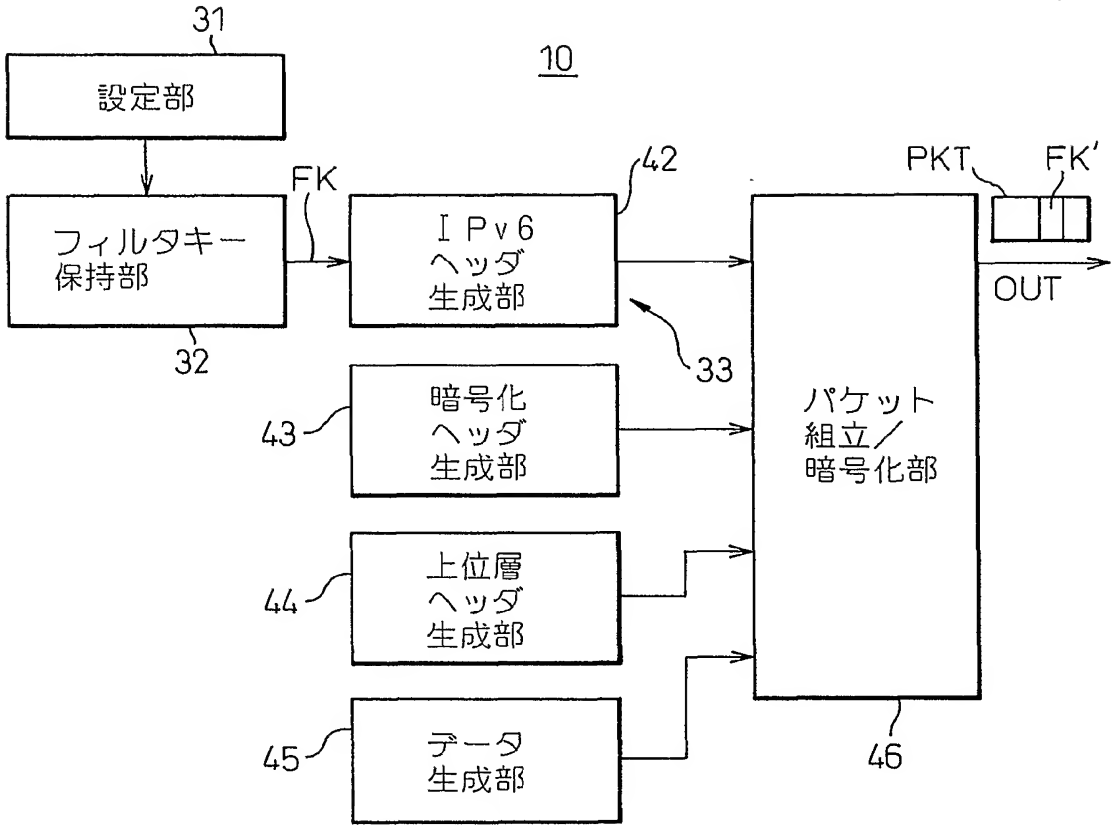

31
10
設定部
FK
フィルタキー
保持部
32
42
IPv6
ヘッダ
生成部
33
PKT
FK'
OUT
暗号化
ヘッダ
生成部
43
上位層
ヘッダ
生成部
44
データ
生成部
45
パケット
組立／
暗号化部
46

Fig.15

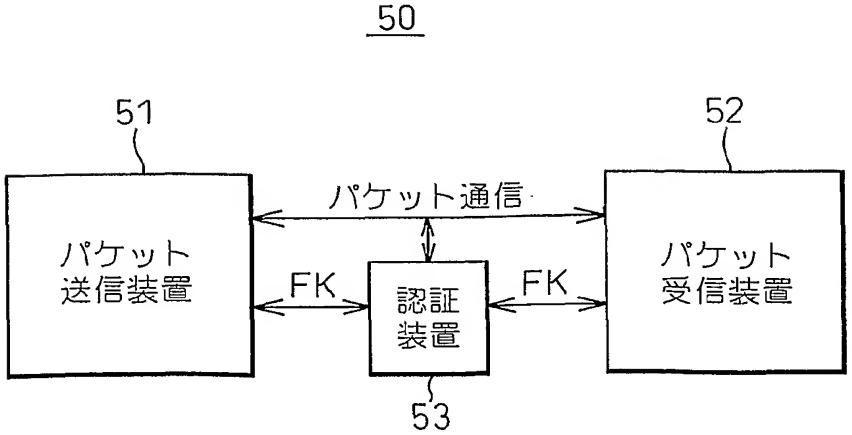

50
51
52
パケット
送信装置
パケット通信
FK
認証
装置
FK
パケット
受信装置
53

Fig.16

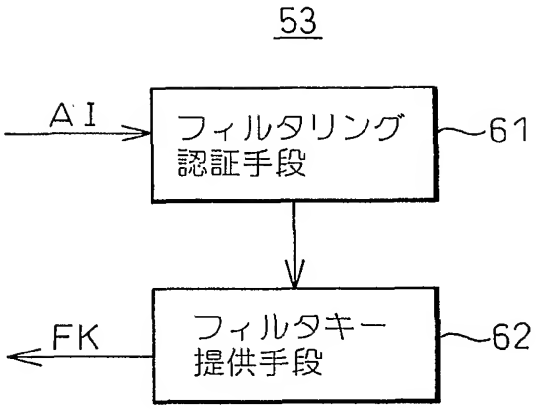

53
AI
フィルタリング
認証手段
61
FK
フィルタキー
提供手段
62

Fig.17

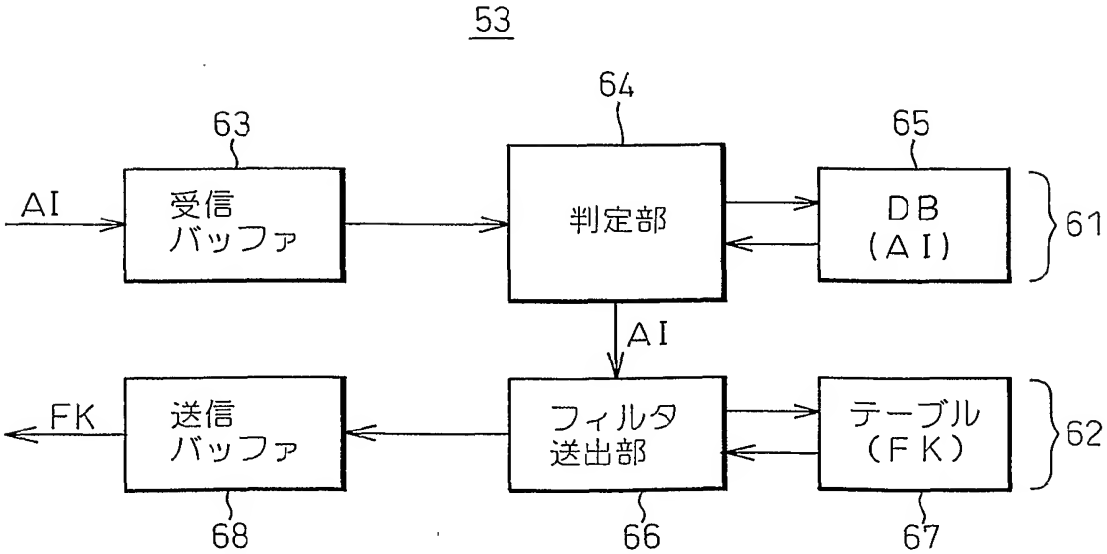

53
64
63
65
AI
受信
バッファ
判定部
DB
(AI)
61
AI
FK
送信
バッファ
フィルタ
送出部
テーブル
(FK)
62
68
66
67

Fig.18

67

AI		FK
ユーザＩＤ①	パスワード①	フィルタキー No. 1
ユーザＩＤ②	パスワード②	フィルタキー No. 2
⋮	⋮	⋮
ユーザＩＤⓝ	パスワードⓝ	フィルタキー No. n

Fig.19

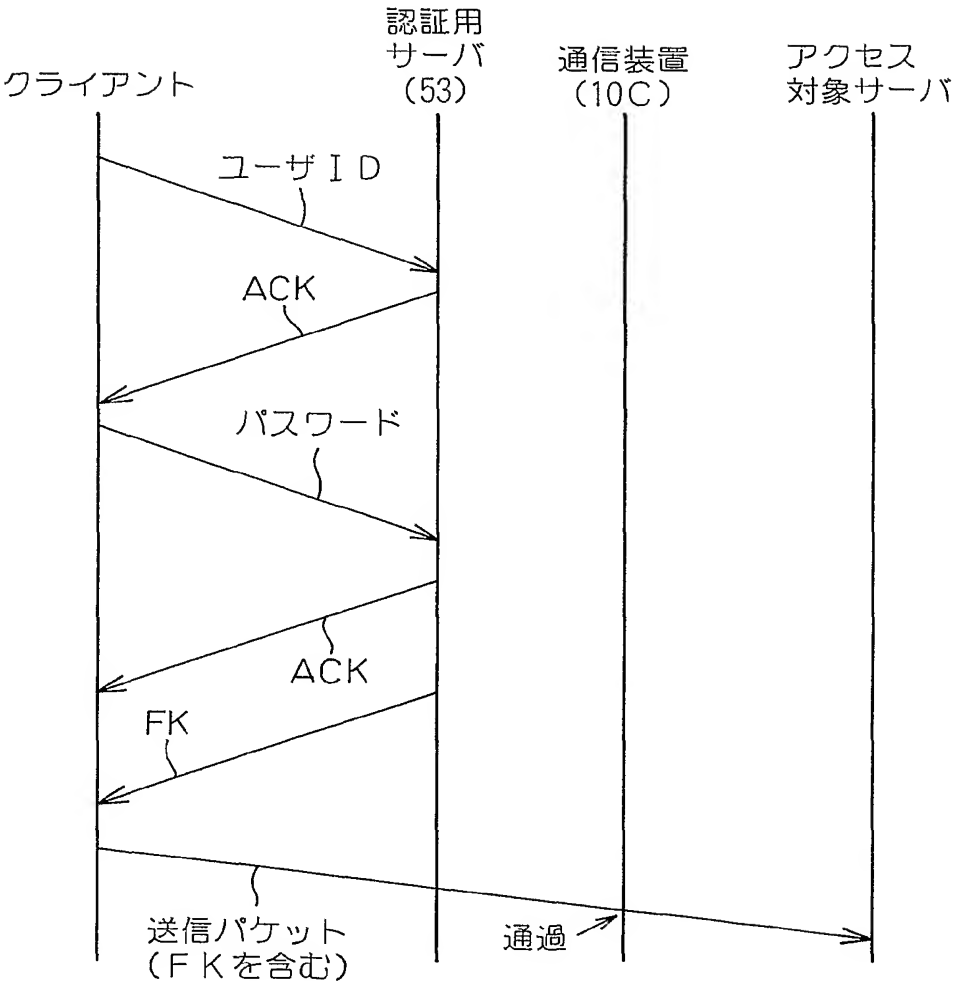

クライアント
認証用
サーバ
(53)
通信装置
(10C)
アクセス
対象サーバ
ユーザＩＤ
ACK
パスワード
ACK
FK
送信パケット
(ＦＫを含む)
通過

Fig.20

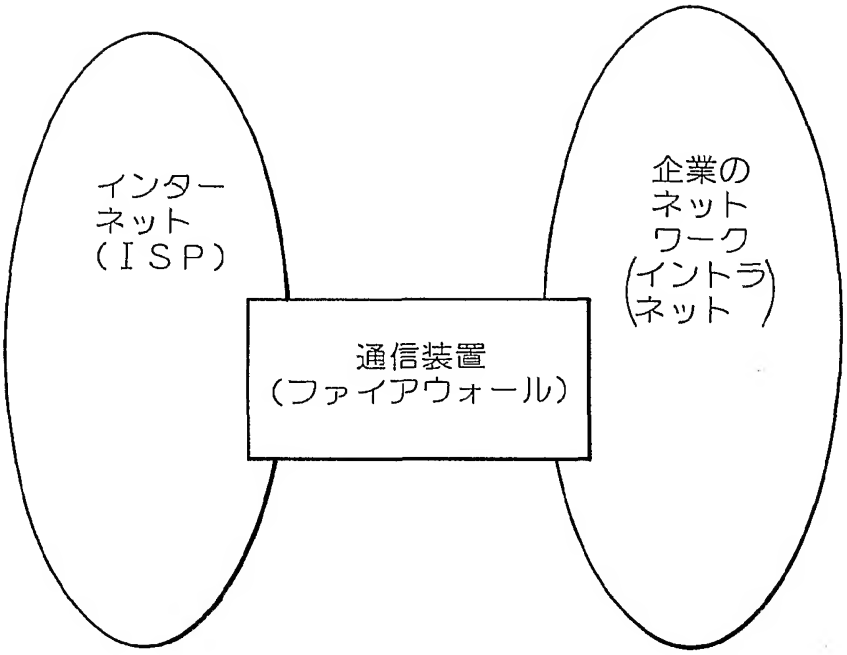

インター
ネット
（ＩＳＰ）
企業の
ネット
ワーク
（イントラ
ネット）
通信装置
（ファイアウォール）

Fig.21

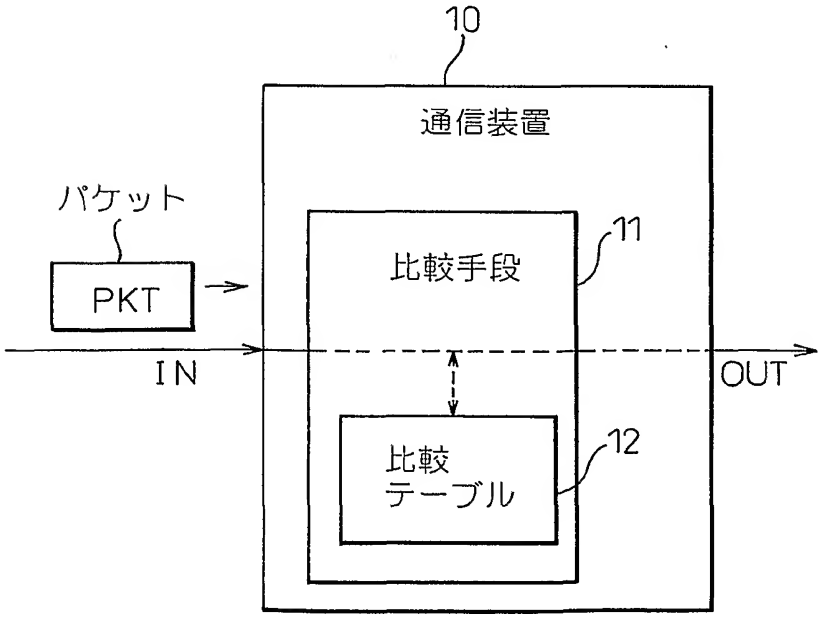

10
通信装置
パケット
PKT
IN
比較手段
11
OUT
比較
テーブル
12

Fig.22

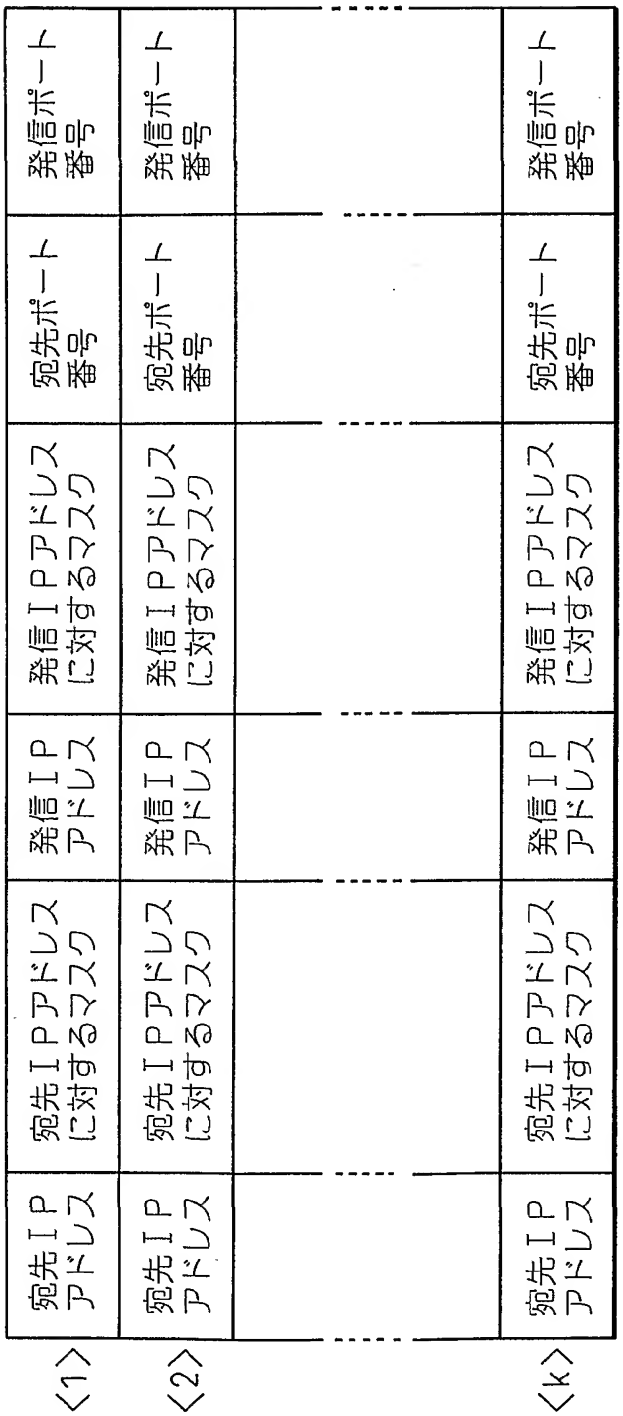

12
<1>
<2>
<k>
宛先ＩＰアドレス
宛先ＩＰアドレスに対するマスク
発信ＩＰアドレス
発信ＩＰアドレスに対するマスク
宛先ポート番号
発信ポート番号

Fig.23

IPv4ヘッダ

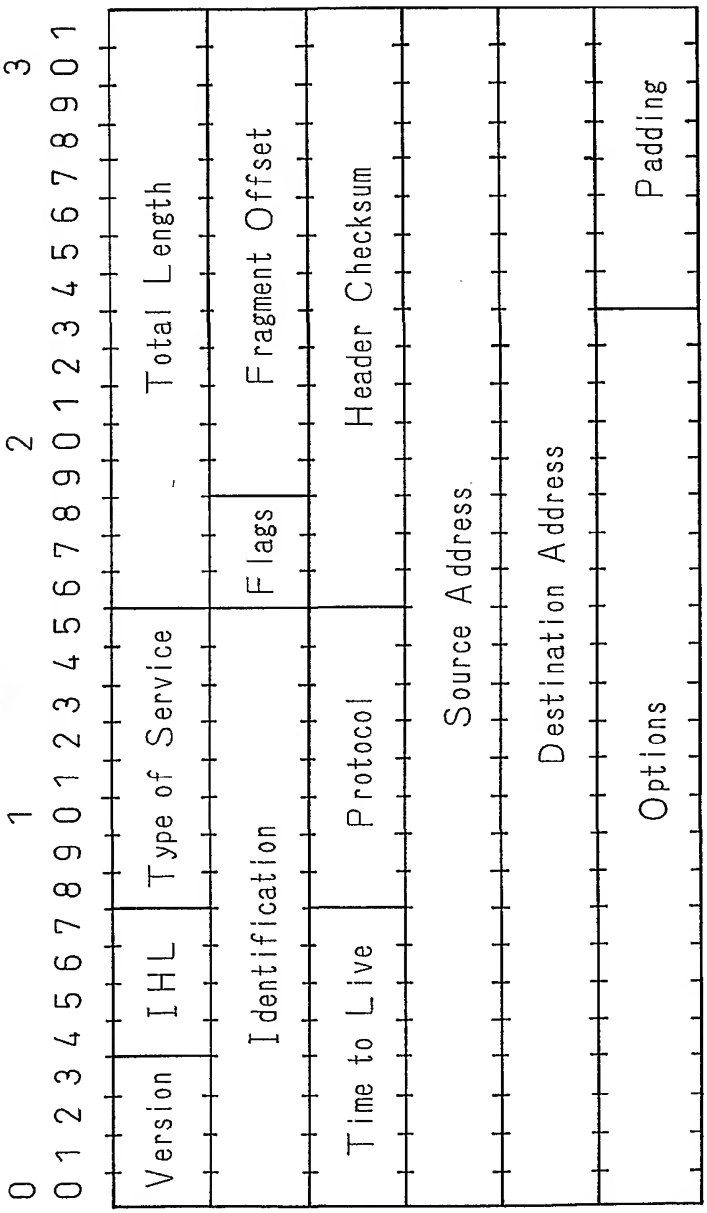


Fig.24

IPv6ヘッダ

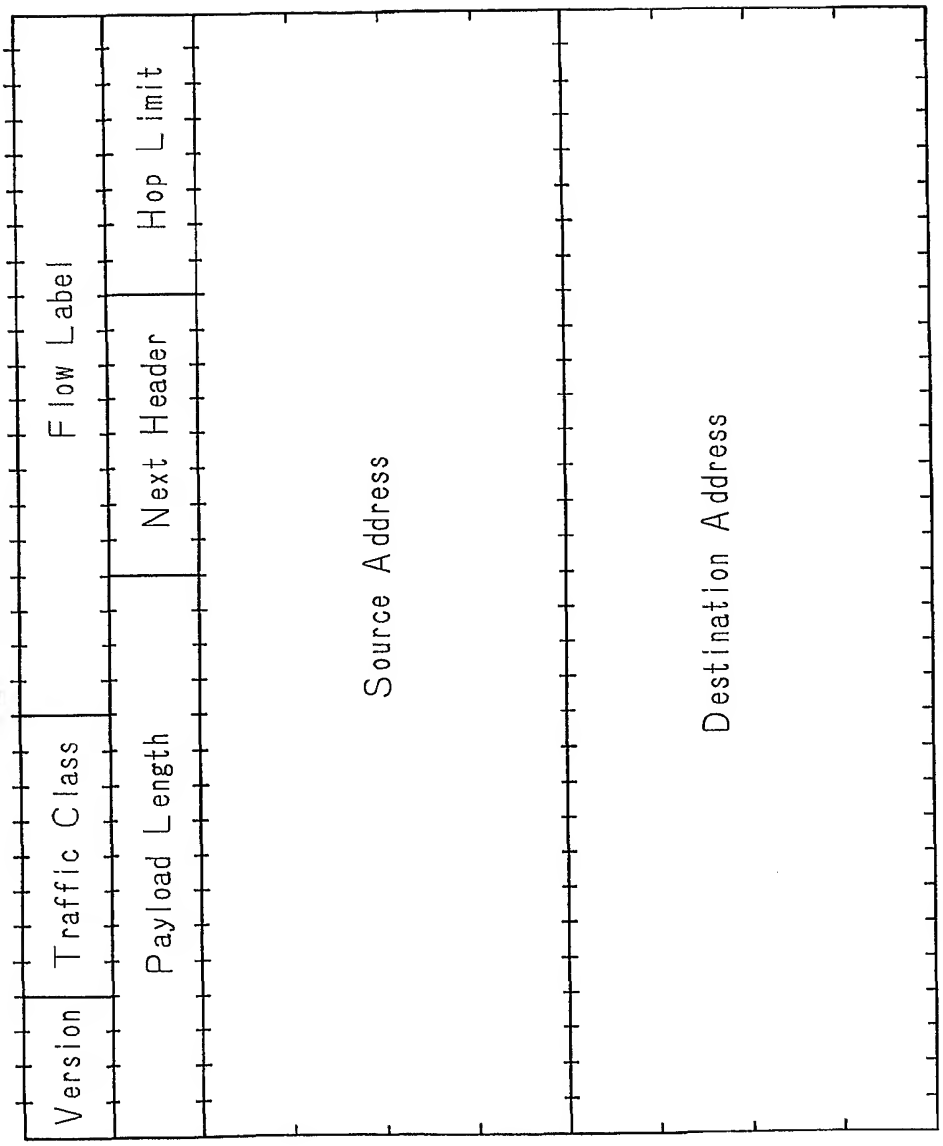


Fig.25

TCPヘッダ

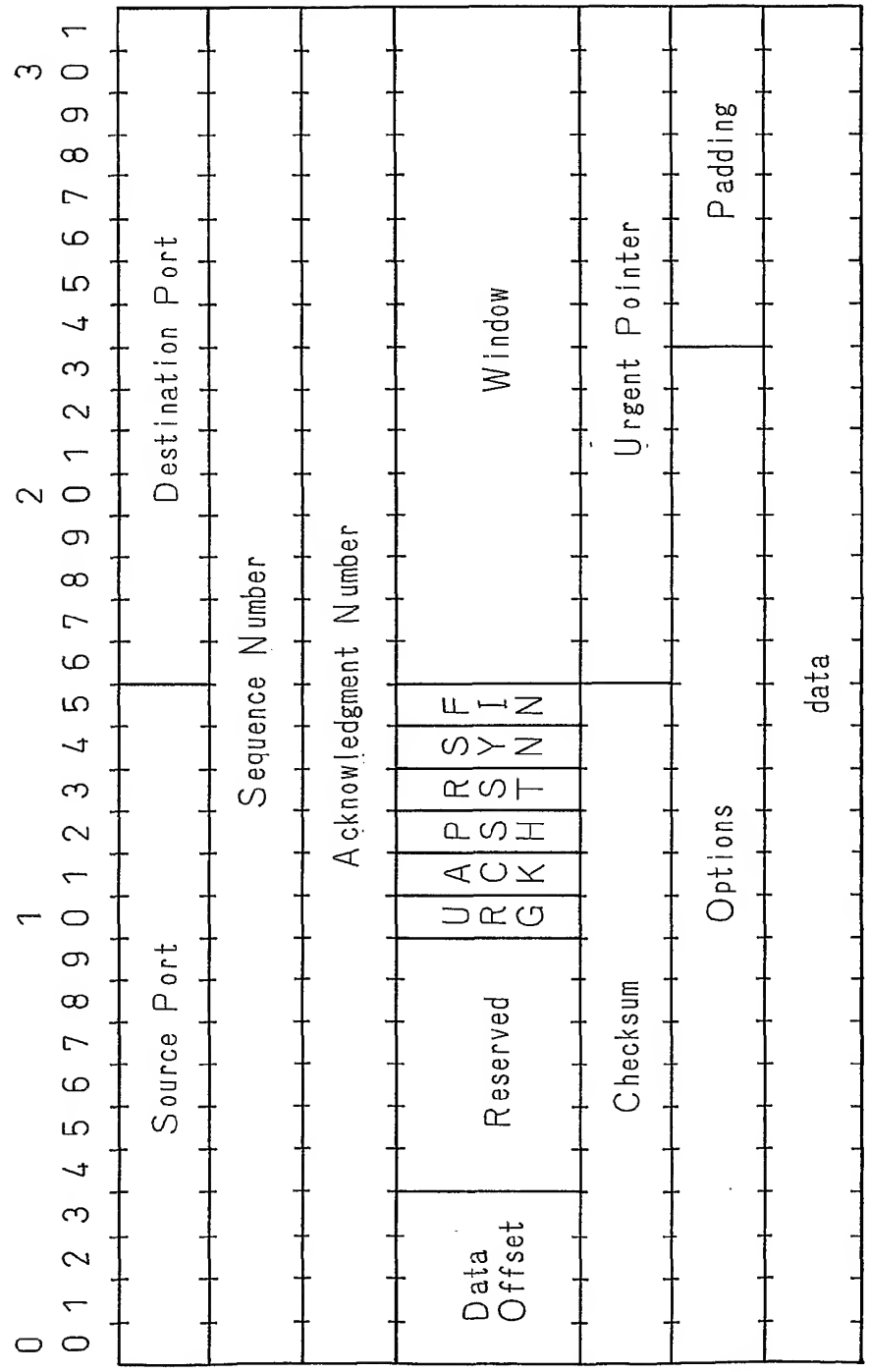


Fig.26

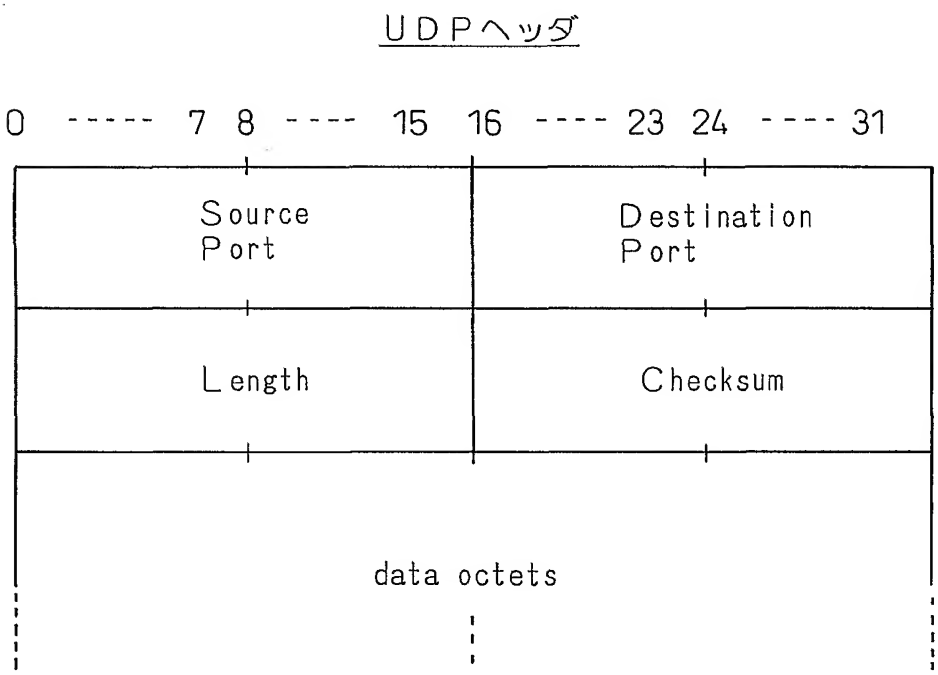
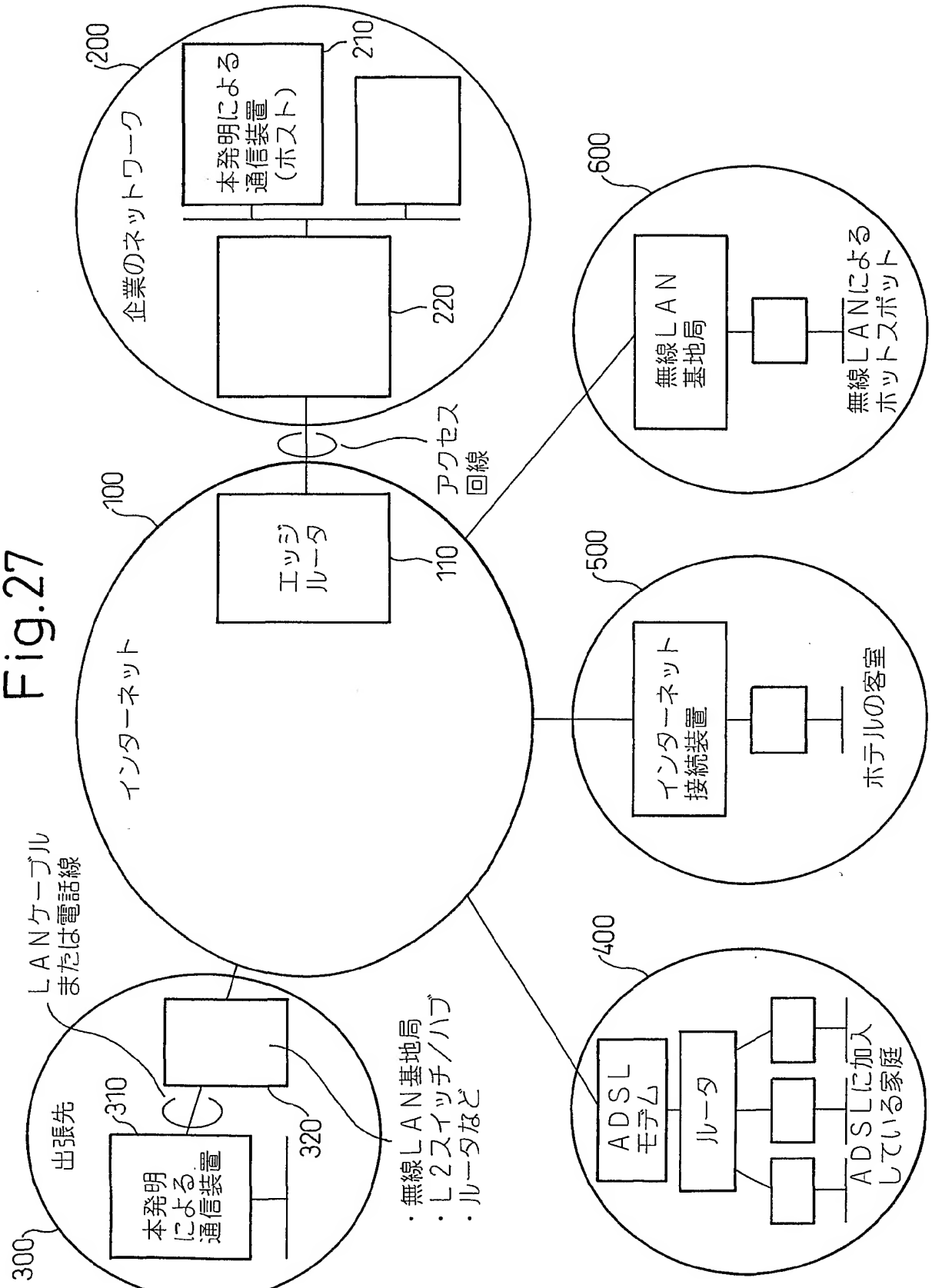

UDPヘッダ
0 ----- 7 8 ---- 15 16 ---- 23 24 ---- 31
Source Port
Destination Port
Length
Checksum
data octets

Fig.27


200
企業のネットワーク
本発明による通信装置（ホスト）
210
220
アクセス回線
100
インターネット
エッジルータ
110
600
無線ＬＡＮ基地局
無線ＬＡＮによるホットスポット
500
インターネット接続装置
ホテルの客室
400
ＡＤＳＬモデム
ルータ
ＡＤＳＬに加入している家庭
300
出張先
ＬＡＮケーブルまたは電話線
310
本発明による通信装置
320
・無線ＬＡＮ基地局
・Ｌ２スイッチ／ハブ
・ルータなど

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/01434

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L12/56, H04L12/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L12/56, H04L12/22, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 6-261057 A (NEC Corp.), 16 September, 1994 (16.09.94), Claim 1; Fig. 1 (Family: none)	1-5 8 6,7,9,10
X Y A	Shinsuke KAWASAKI, "Mitsubishi Shoji 20 Sha o Musubu Extra Net Ninsho·Angoka ha Gaibu ni Itaku", Nikkei Communication, No.288, pages 131 to 136; Nikkei Business Publications, Inc., 15 February, 1999 (15.02.99), (CS-ND-1999-00487-004) Page 134, central column, line 5 to page 135,left column, line 15; Fig. 2	6,9,10 7,8 1-5
Y A	JP 2000-59357 A (Nippon Telegraph And Telephone Corp.), 25 February, 2000 (25.02.00), Par. Nos. [0013] to [0031]; Figs. 1, 7, 8 (Family: none)	7 1-6,8-10

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
19 April, 2002 (19.04.02)

Date of mailing of the international search report
30 April, 2002 (30.04.02)

Name and mailing address of the ISA/
Japanese Patent Office

Facsimile No.

Authorized officer

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/01434

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 10-233795 A (Nippon Telegraph And Telephone Corp.), 02 September, 1998 (02.09.98), Par. Nos. [0015], [0017]; Fig. 3 (Family: none)	1-10
A	JP 9-214556 A (Toshiba Corp.), 15 August, 1997 (15.08.97), Full text; all drawings & US 6092191 A & US 6185680 B1	1-10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/01434

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-5, 8 define the invention of storing filtering information in a packet and transmitting it on the transmission side, and executing packet filtering based on the filtering information on the receiving side.

Claims 6, 7, 9, 10 define the invention that an authenticating apparatus receives authenticating information input by a user and provides a filter key corresponding with the authenticating information to this user.

These inventions are not united into oneinvention nor so linked as to form a single inventive general concept.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０１４３４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ．[7]　Ｈ０４Ｌ　１２／５６，Ｈ０４Ｌ　１２／２２

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ．[7]　Ｈ０４Ｌ　１２／５６，Ｈ０４Ｌ　１２／２２，Ｈ０４Ｌ　９／３２

最小限資料以外の資料で調査を行った分野に含まれるもの

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　６－２６１０５７　Ａ（日本電気株式会社） １９９４．０９．１６ 【請求項１】，【図１】 （ファミリなし）	１－５
Ｙ		８
Ａ		６，７，９，１０

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１９．０４．０２	30.04.02

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	間野　裕一	５Ｘ　９７４４
	電話番号　０３－３５８１－１１０１　内線　３５９４	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	川崎慎介，「三菱商事　２０社を結ぶエクストラネット　認証・暗号化は外部に委託」，日経コミュニケーション，第２８８号，第１３１－１３６頁，日経ＢＰ社，１９９９．０２．１５ (CS-ND-1999-00487-004) 第１３４頁中央欄第５行－第１３５頁左欄第１５行，図２	６，９，１０
Ｙ		７，８
Ａ		１－５
Ｙ	ＪＰ　２０００－５９３５７　Ａ（日本電信電話株式会社） ２０００．０２．２５ 【００１３】－【００３１】，【図１】，【図７】，【図８】 （ファミリなし）	７
Ａ		１－６， ８－１０
Ａ	ＪＰ　１０－２３３７９５　Ａ（日本電信電話株式会社） １９９８．０９．０２ 【００１５】，【００１７】，【図３】 （ファミリなし）	１－１０
Ａ	ＪＰ　９－２１４５５６　Ａ（株式会社東芝） １９９７．０８．１５ 全文，全図 &ＵＳ　６０９２１９１　Ａ &ＵＳ　６１８５６８０　Ｂ１	１－１０

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０１４３４

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲１－５，８は、送信側においてパケットにフィルタリング情報を格納して送信し、受信側において該フィルタリング情報をもとにパケットフィルタリングを実施する発明である。
一方、請求の範囲６，７，９，１０は、認証装置がユーザから入力された認証情報を受信して、該ユーザに対し該認証情報に対応するフィルタキーを提供する発明である。
これらは、一の発明であるとも、単一の一般的発明概念を形成するように連関している一群の発明であるとも認められない。

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。